Fundamentals of Phishing: A Usability Perspective

Zane Ma

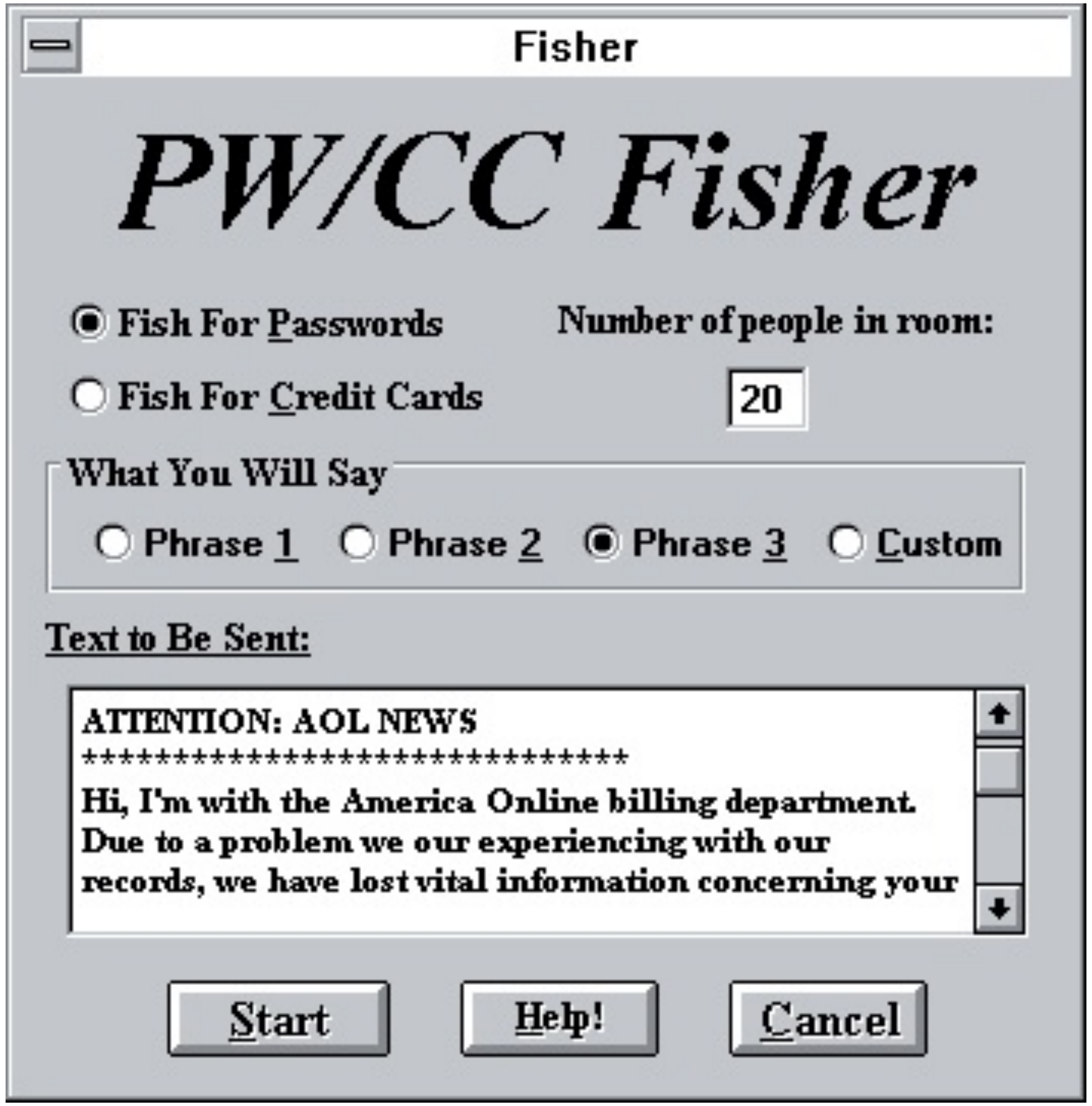
University of Illinois Urbana-Champaign

zanema2@illinois.edu
https://zanema.com

Phishing: Roots

AOL *Instant Messenger*℠

1995 - AOL cracking tool



Fisher

PW/CC Fisher

● Fish For Passwords

○ Fish For Credit Cards

Number of people in room: 20

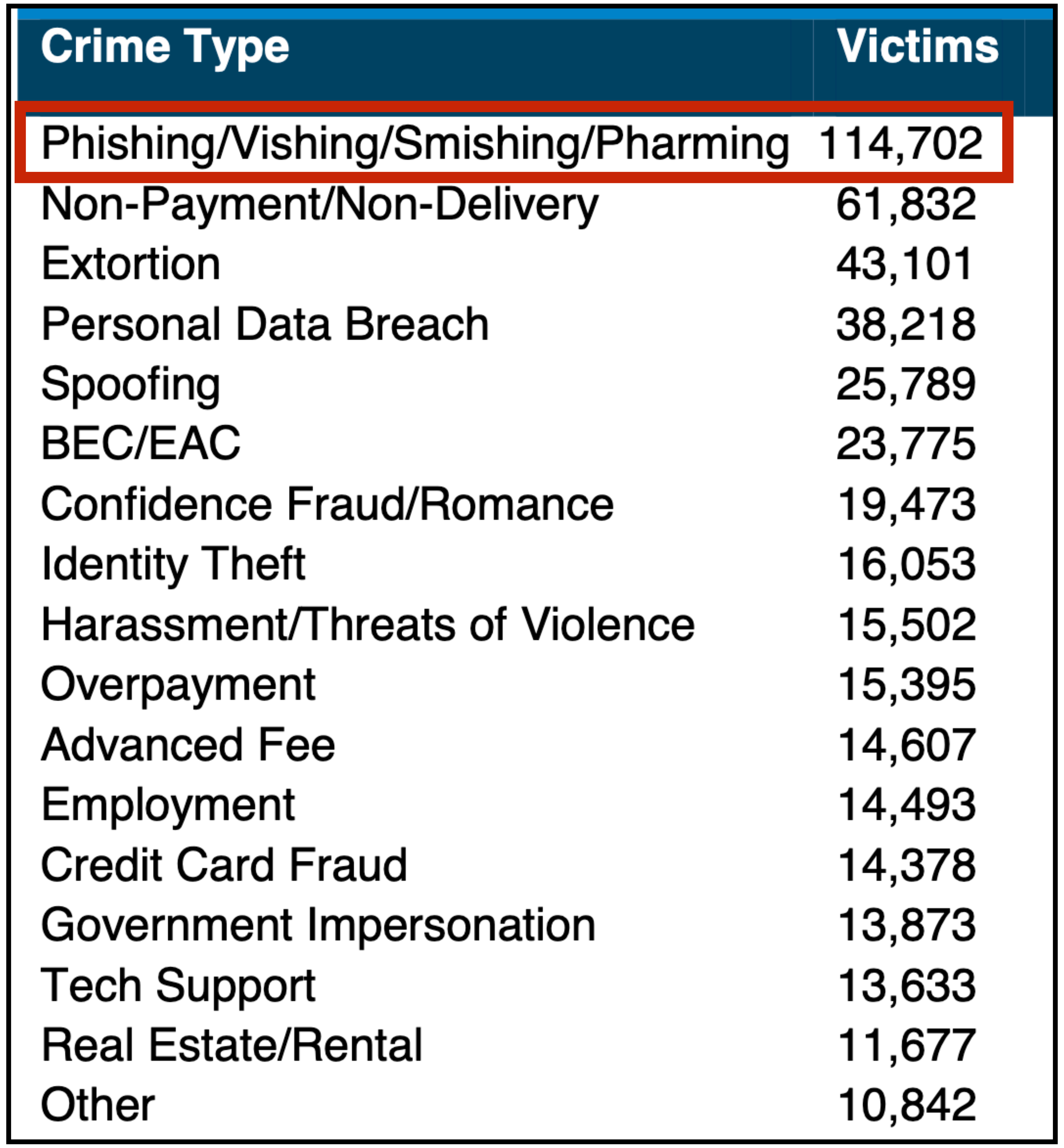
What You Will Say

○ Phrase 1 ○ Phrase 2 ● Phrase 3 ○ Custom

Text to Be Sent:

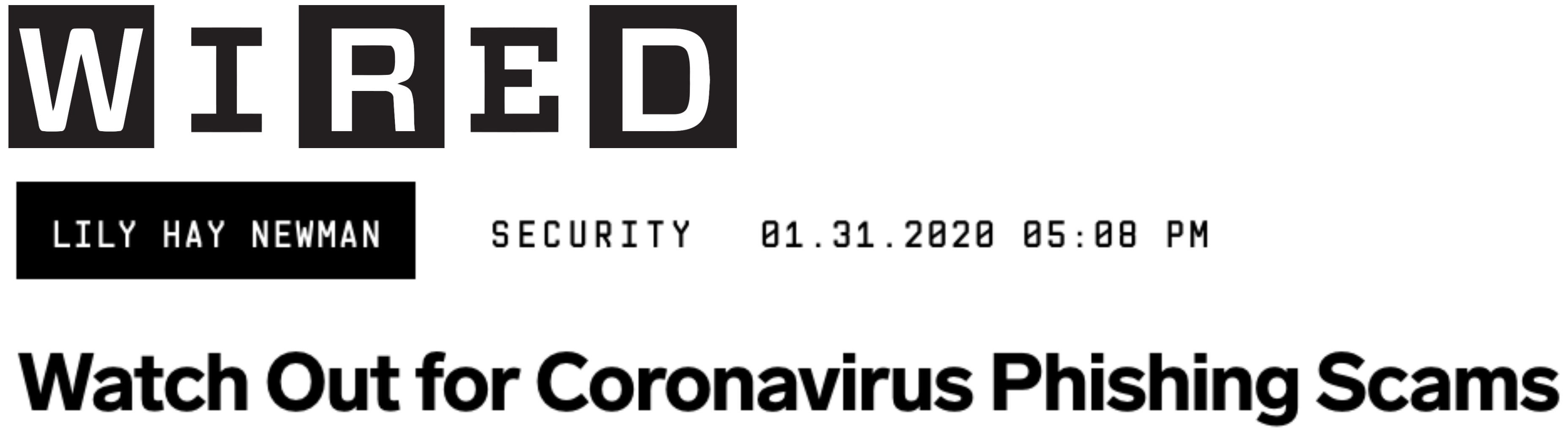
ATTENTION: AOL NEWS
****
Hi, I'm with the America Online billing department. Due to a problem we our experiencing with our records, we have lost vital information concerning your

Phishing: Today



Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	114,702
Non-Payment/Non-Delivery	61,832
Extortion	43,101
Personal Data Breach	38,218
Spoofing	25,789
BEC/EAC	23,775
Confidence Fraud/Romance	19,473
Identity Theft	16,053
Harassment/Threats of Violence	15,502
Overpayment	15,395
Advanced Fee	14,607
Employment	14,493
Credit Card Fraud	14,378
Government Impersonation	13,873
Tech Support	13,633
Real Estate/Rental	11,677
Other	10,842

Source: 2019 FBI Internet Crime Report

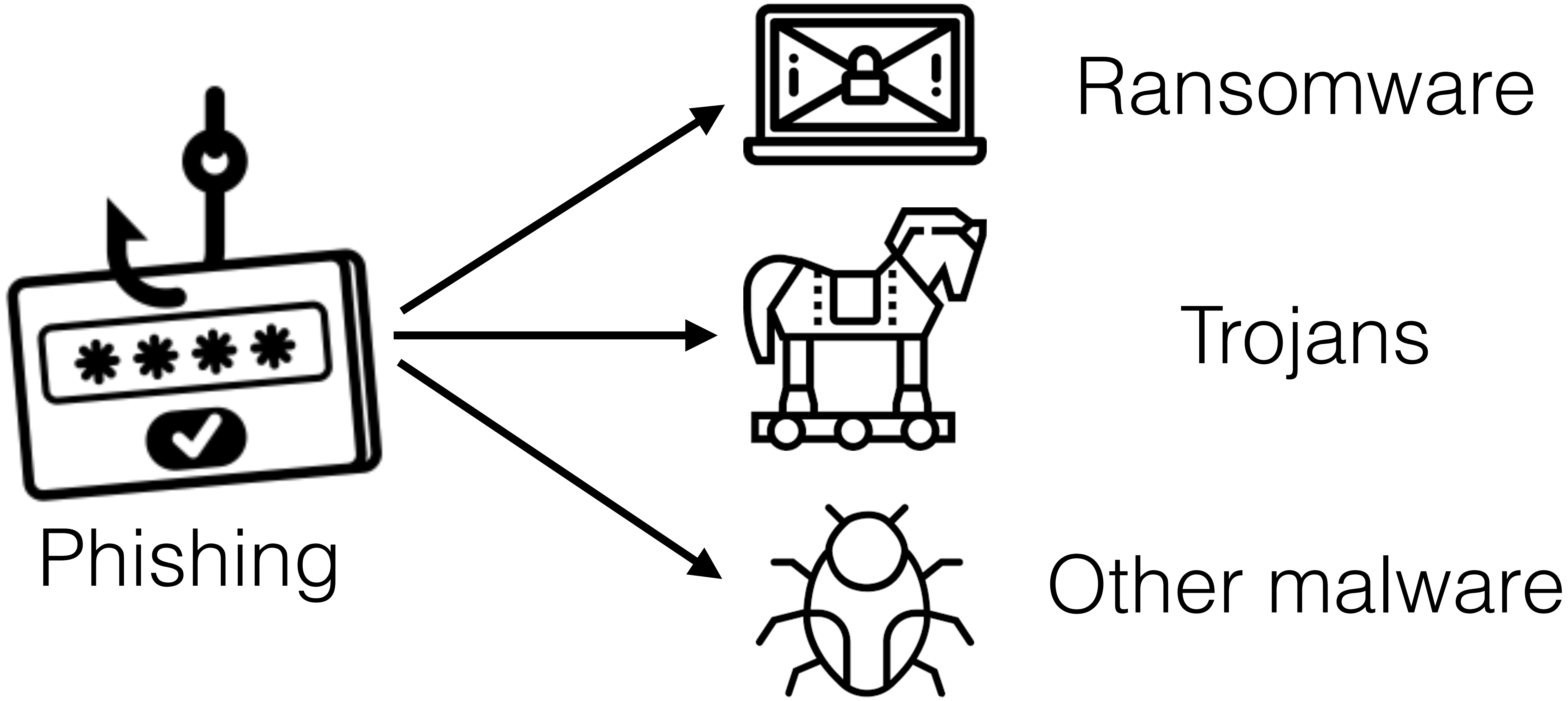


WIRED

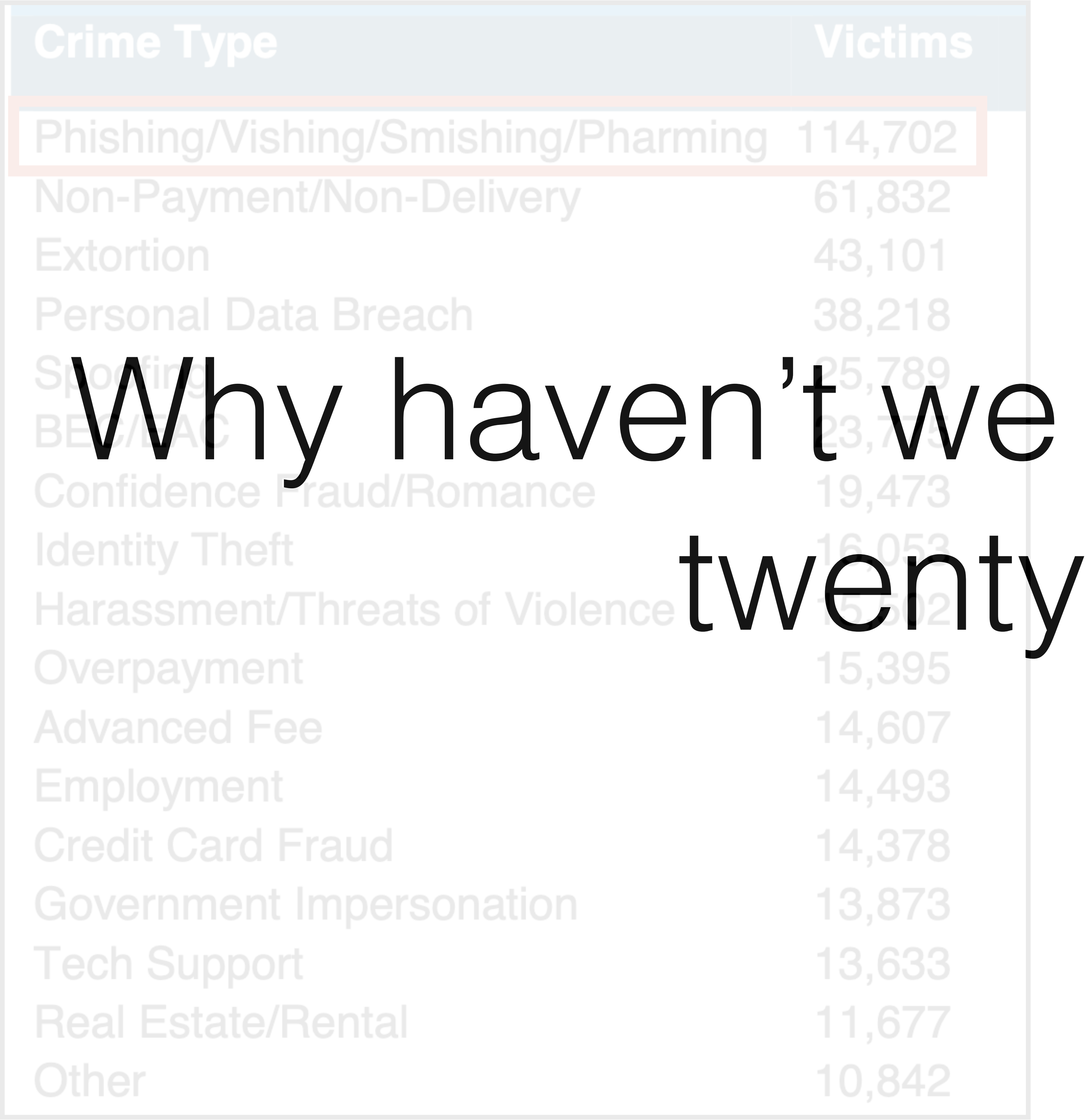
LILY HAY NEWMAN SECURITY 01.31.2020 05:00 PM

Watch Out for Coronavirus Phishing Scams

2016 DEMOCRATIC NATIONAL CONVENTION



Phishing: Today



Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	114,702
Non-Payment/Non-Delivery	61,832
Extortion	43,101
Personal Data Breach	38,218
Spoofing	25,789
BEC/EAC	23,775
Confidence Fraud/Romance	19,473
Identity Theft	16,053
Harassment/Threats of Violence	15,502
Overpayment	15,395
Advanced Fee	14,607
Employment	14,493
Credit Card Fraud	14,378
Government Impersonation	13,873
Tech Support	13,633
Real Estate/Rental	11,677
Other	10,842

Source: 2019 FBI Internet Crime Report

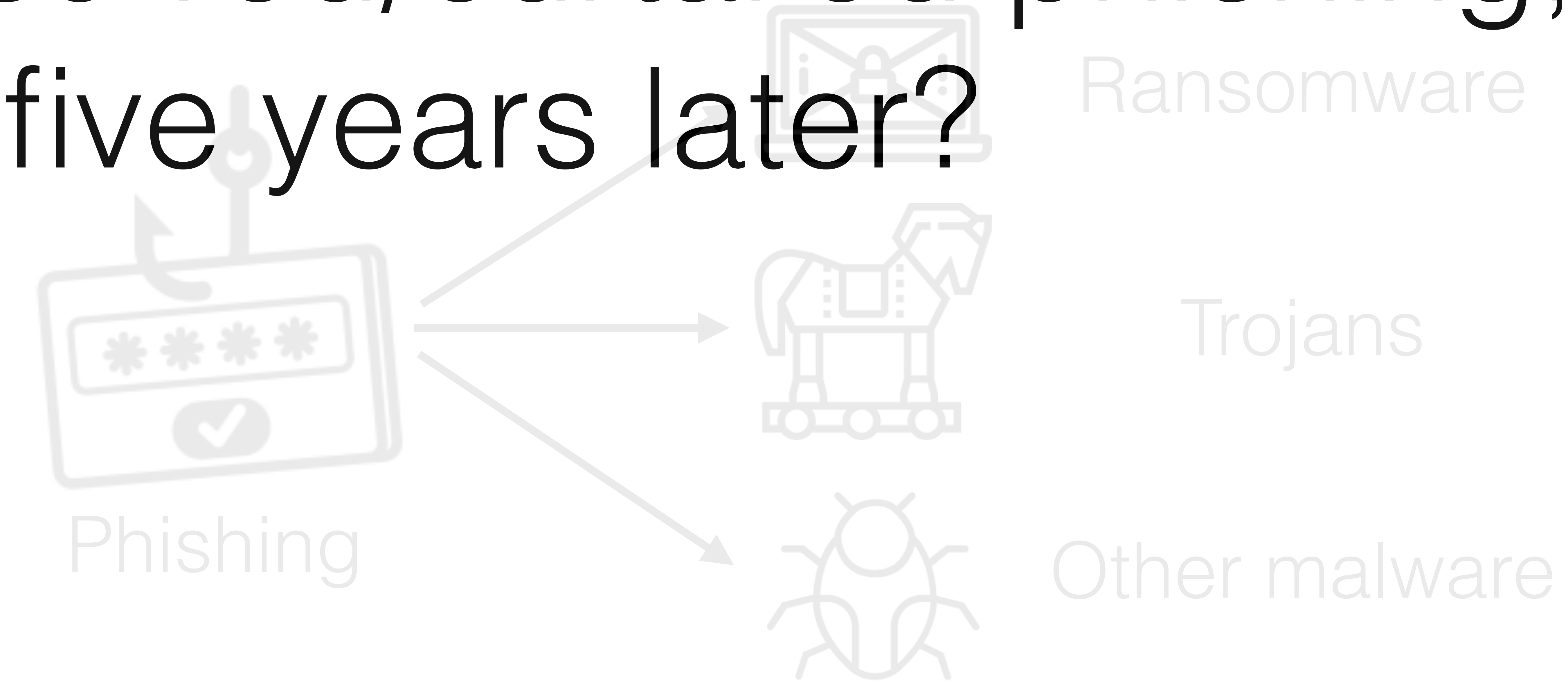
WIRED

LILY HAY NEWMAN SECURITY 01.31.2020 05:00 PM

Watch Out for Coronavirus Phishing Scams

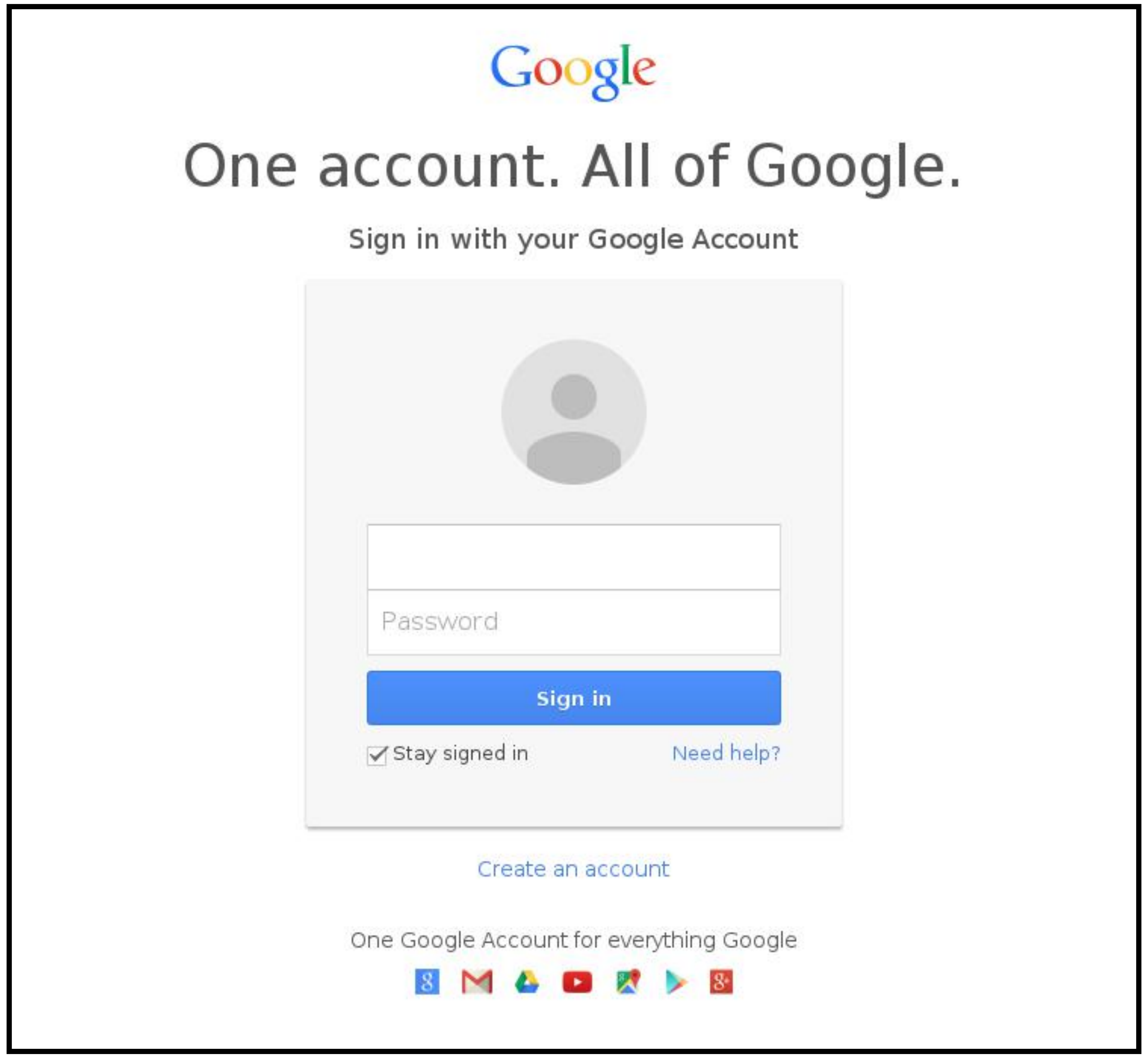
2016 DEMOCRATIC NATIONAL CONVENTION

Why haven't we solved/curtailed phishing, twenty-five years later?



Phishing: Root Causes

Mistaken Identity



Google

One account. All of Google.

Sign in with your Google Account

Password

☑ Stay signed in

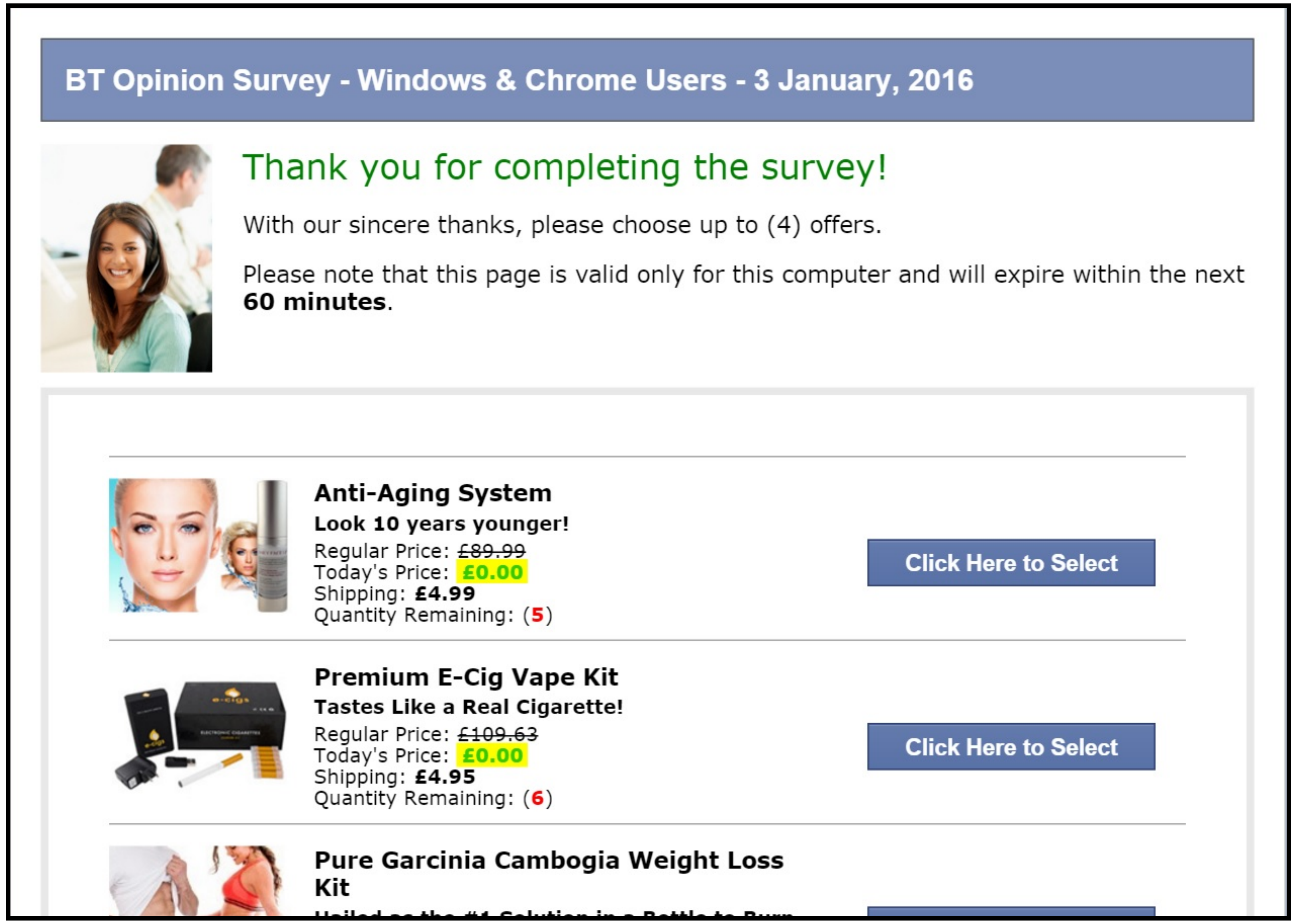
Need help?

Create an account

One Google Account for everything Google

accoounts-google.com

Misplaced Trust



BT Opinion Survey - Windows & Chrome Users - 3 January, 2016

Thank you for completing the survey!

With our sincere thanks, please choose up to (4) offers.

Please note that this page is valid only for this computer and will expire within the next **60 minutes**.

Anti-Aging System
Look 10 years younger!
Regular Price: ~~£89.99~~
Today's Price: **£0.00**
Shipping: **£4.99**
Quantity Remaining: (**5**)

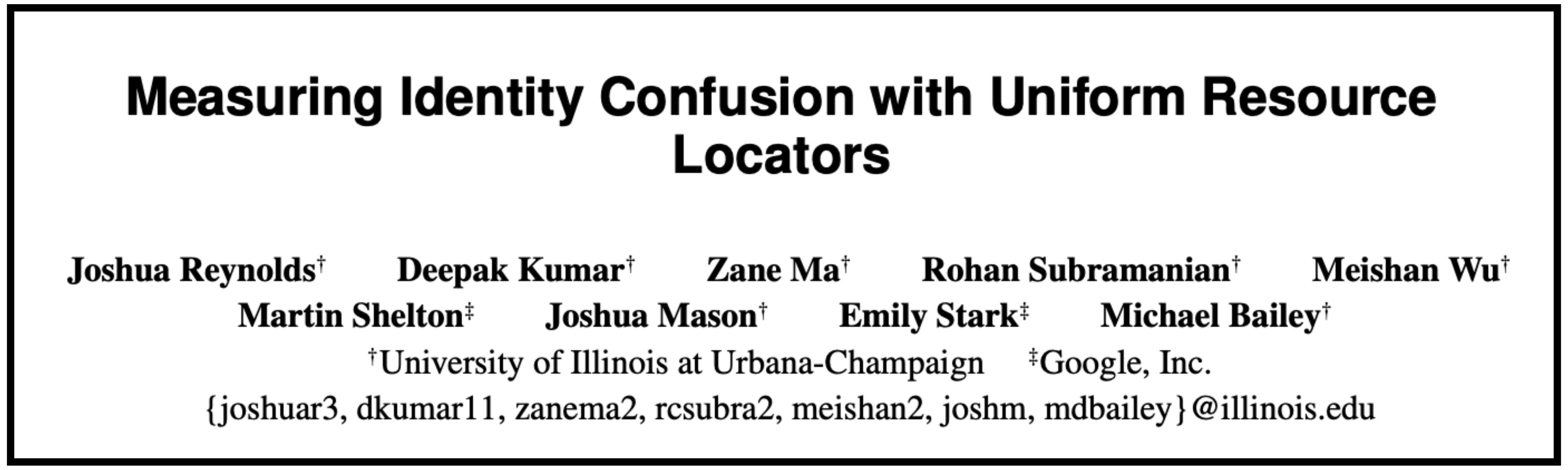
Premium E-Cig Vape Kit
Tastes Like a Real Cigarette!
Regular Price: ~~£109.63~~
Today's Price: **£0.00**
Shipping: **£4.95**
Quantity Remaining: (**6**)

Pure Garcinia Cambogia Weight Loss Kit
Hailed as the #1 Solution in a Bottle to Burn

questionsaboutisps.com

Phishing: Root Causes

Mistaken Identity



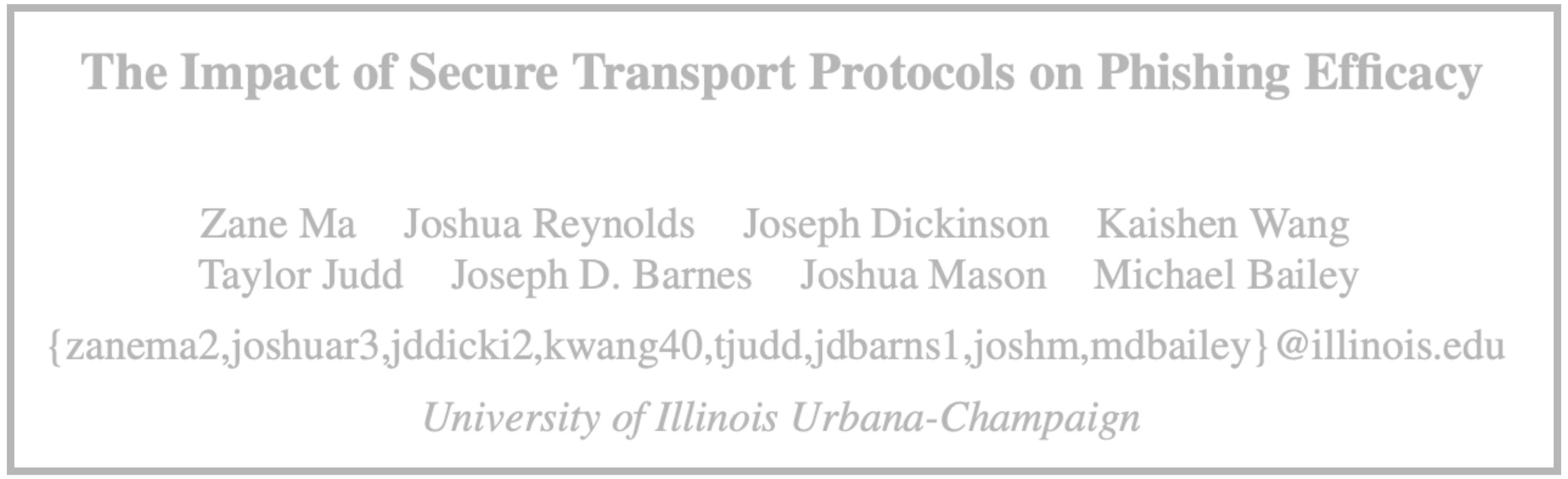
Measuring Identity Confusion with Uniform Resource Locators

Joshua Reynolds[†] Deepak Kumar[†] Zane Ma[†] Rohan Subramanian[†] Meishan Wu[†]
Martin Shelton[‡] Joshua Mason[†] Emily Stark[‡] Michael Bailey[†]
[†]University of Illinois at Urbana-Champaign [‡]Google, Inc.
{joshuar3, dkumar11, zanema2, rcsubra2, meishan2, joshm, mdbailey}@illinois.edu

CHI 2020

URL complexity leads to mistaken identity

Misplaced Trust



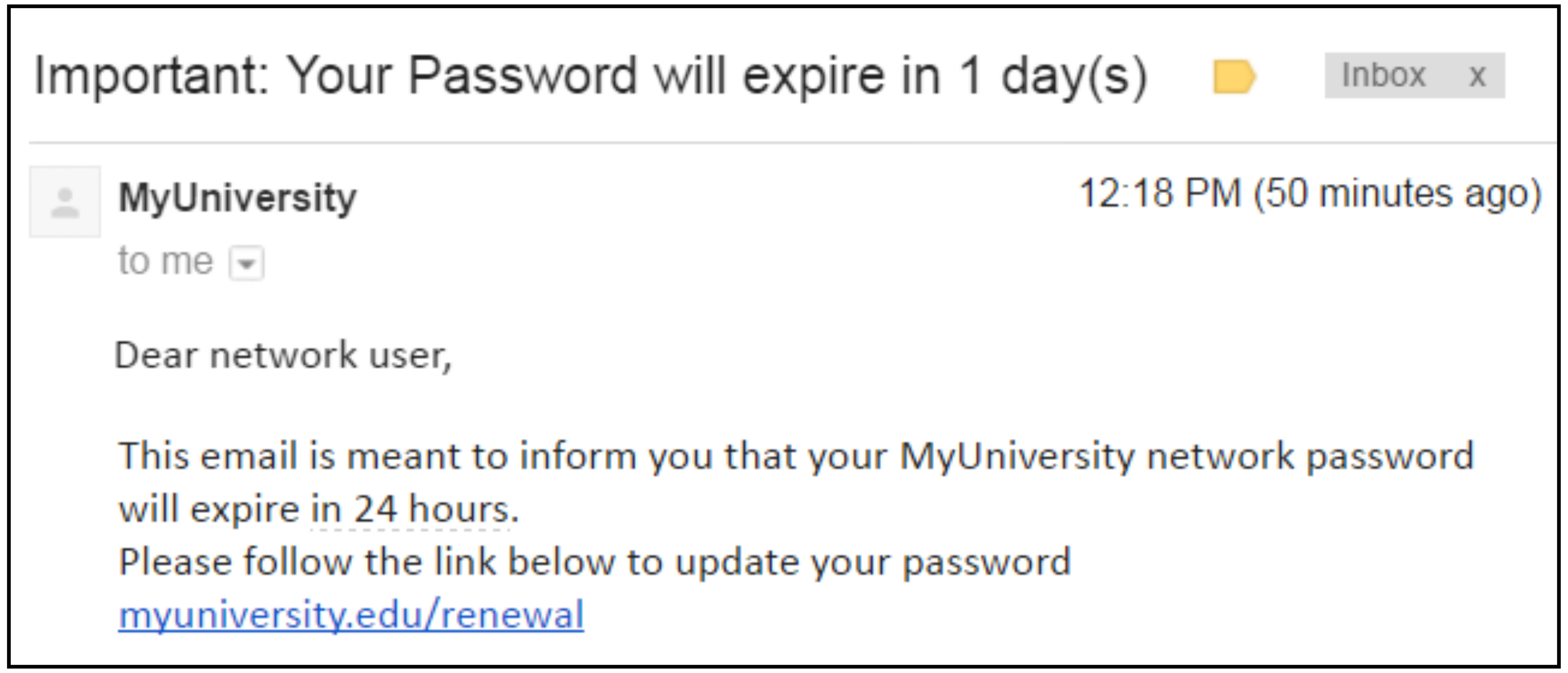
The Impact of Secure Transport Protocols on Phishing Efficacy

Zane Ma Joshua Reynolds Joseph Dickinson Kaishen Wang
Taylor Judd Joseph D. Barnes Joshua Mason Michael Bailey
{zanema2,joshuar3,jddicki2,kwang40,tjudd,jdbarns1,joshm,mdbailey}@illinois.edu
University of Illinois Urbana-Champaign

CSET 2019

Users may (mis)place trust in HTTPS

Ubiquitous URLs



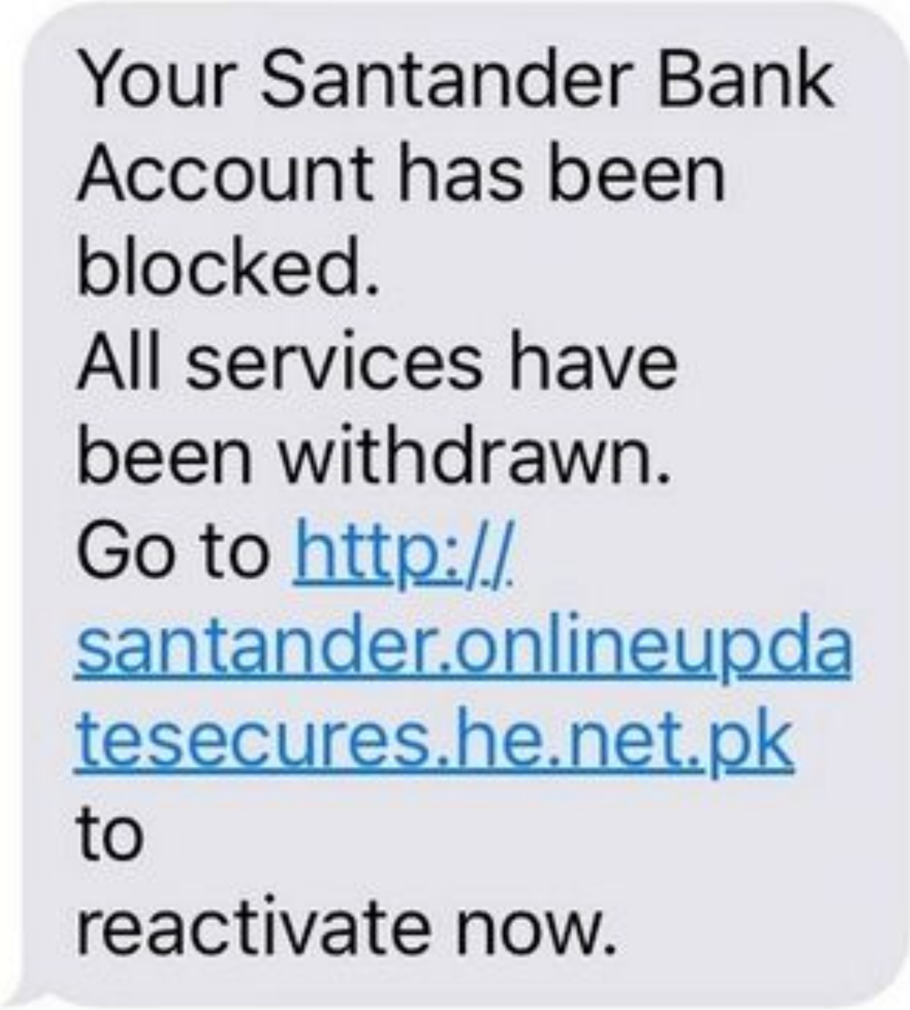
Important: Your Password will expire in 1 day(s)

MyUniversity 12:18 PM (50 minutes ago)

to me

Dear network user,

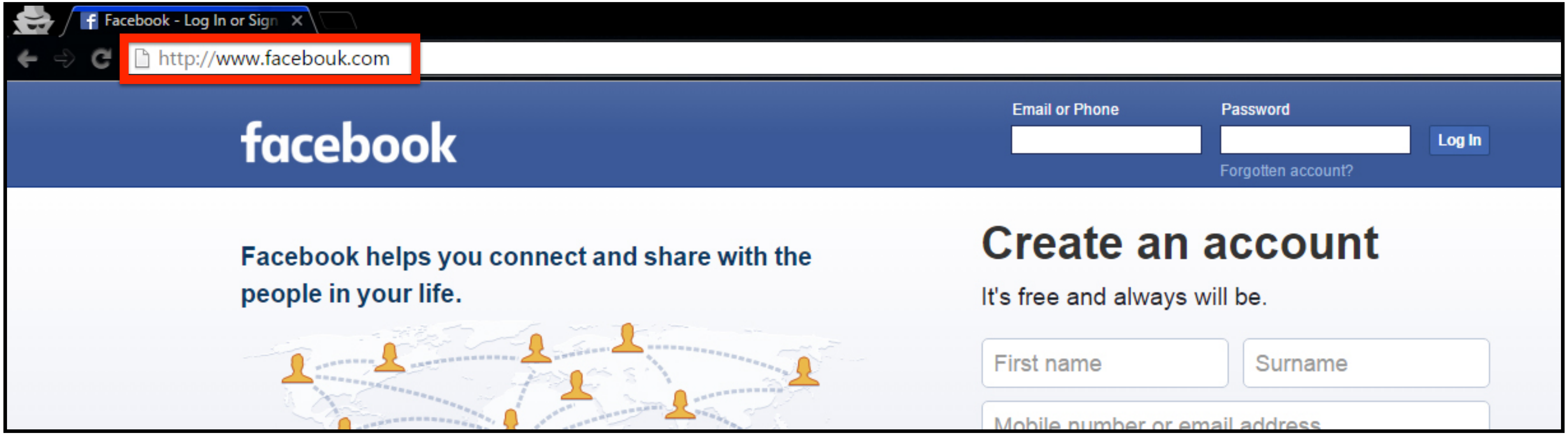
This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal



Your Santander Bank Account has been blocked.
All services have been withdrawn.
Go to http://santander.onlineupdatesecures.he.net.pk to reactivate now.

hanes.com/briefs

URLs in Browsers



http://www.facebouk.com

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

Everything is trivially spoofable besides the URL

URL Complexity

What is the second-level domain + TLD?

http://example.com

https://paypal.com.accounts.ggle.com/signin/v2/identifier?service=accountsettings&hl=en-US&continue=https%3A%2F%2Fmyaccount.google.com

https://fb.com∕login@example.com%2e2e2e2e2e%2emx?@bofa.com/login.php#twitter.com

URL Complexity

What is the second-level domain + TLD?

http://**example.com**

https://paypal.com.accounts.**ggle.com**/signin/v2/identifier?service=accountsettings&hl=en-US&continue=https%3A%2F%2Fmyaccount.google.com

https://fb.com∕login@example.com.**2e2e2e2e.mx**?@bofa.com/login.php#twitter.com

Research Questions

Given that URLs are ubiquitous and complex:

1. How well do users parse identity information from URLs?
2. What URL features or user strategies lead to mistakes?

94 Mechanical Turk participants

User Confidence

“I know how to read a URL”

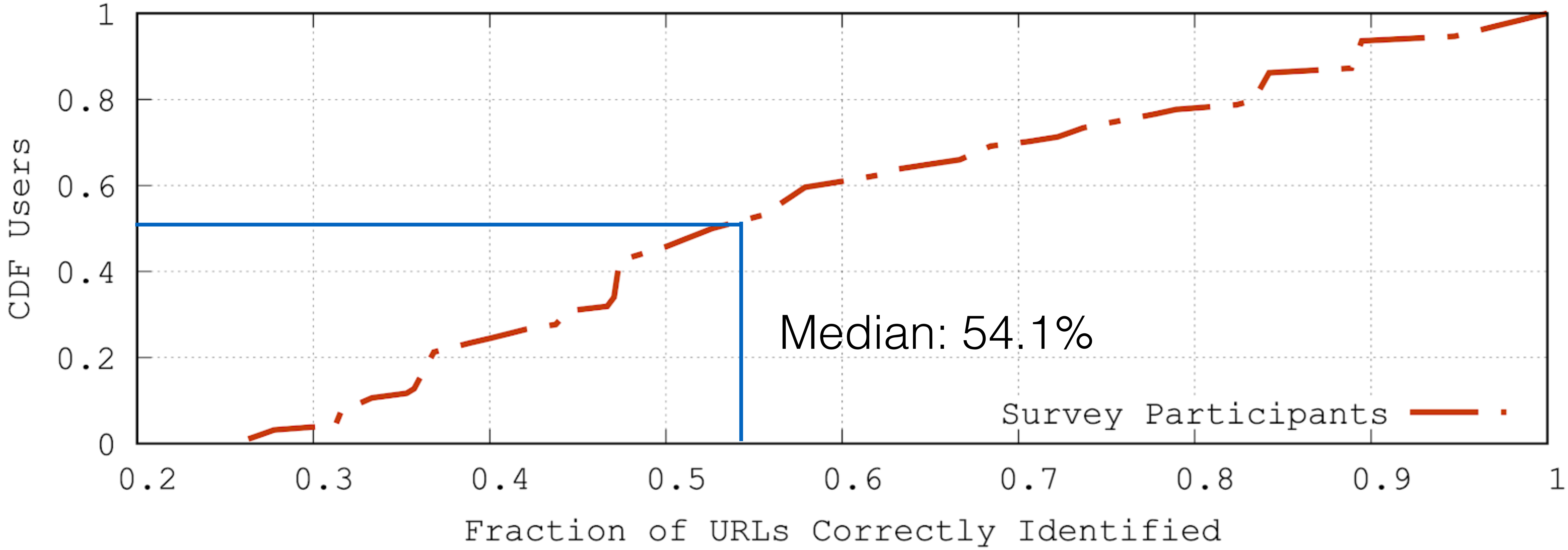
- 91/94 reported “Very True” or “Mostly True”

“I know how to tell what website I am on”

- 91/94 reported “Very True” or “Mostly True”

Target Identification

Asked users to describe the target of 19-20 URLs, some with one of 13 different URL obfuscations applied



Research Questions

Given that URLs are ubiquitous and complex:

1. How well do users parse identity information from URLs?

   - Poorly (54% median accuracy), despite user confidence

2. What URL features or user strategies lead to mistakes?

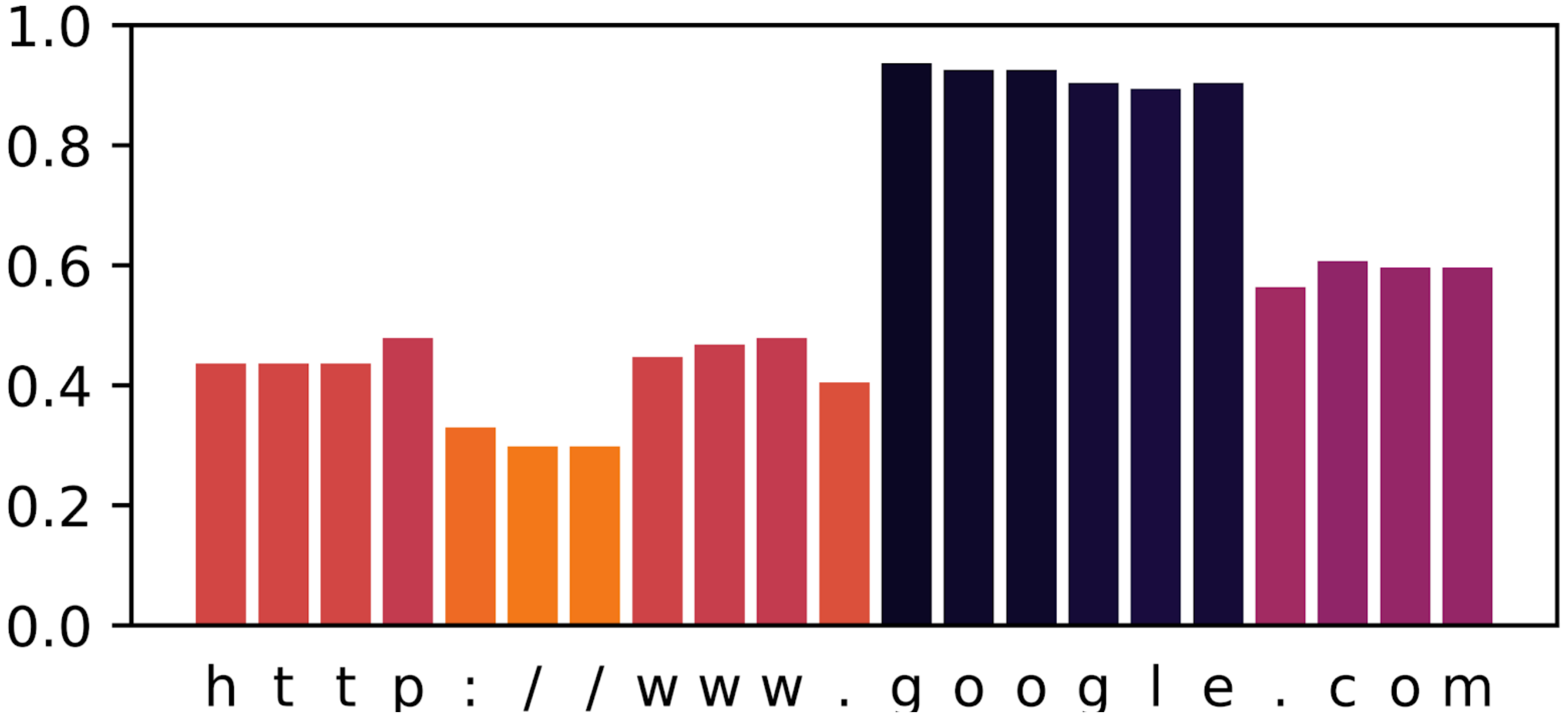
URL Obfuscation

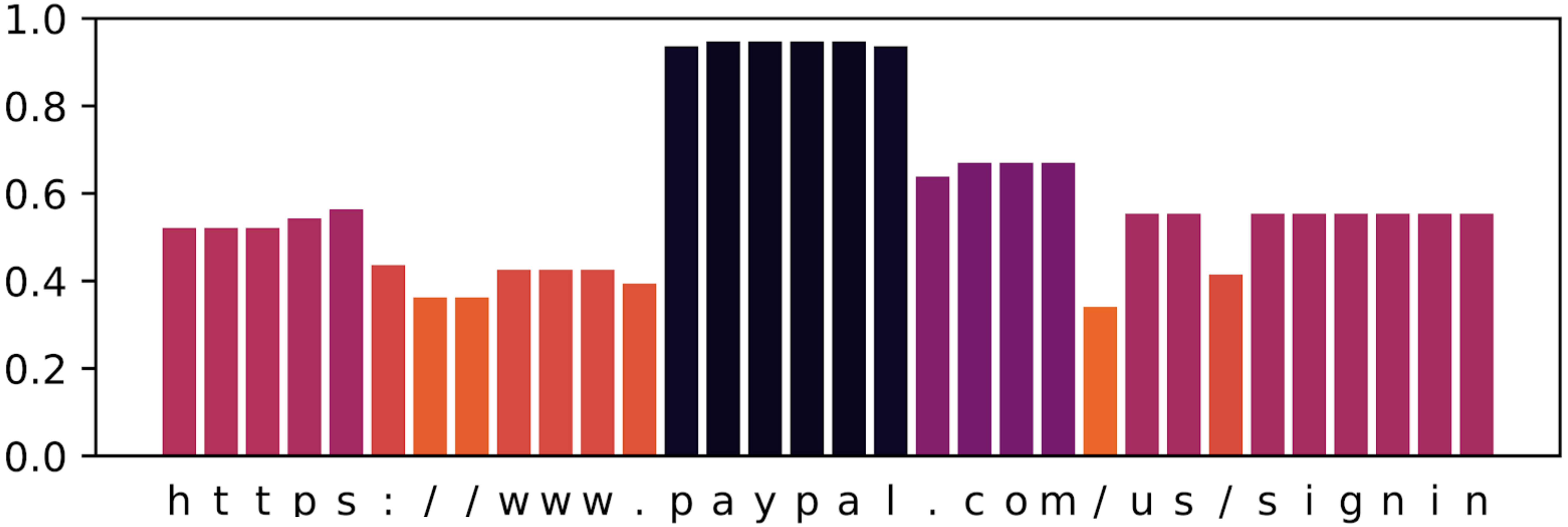
Unobfuscated URLs 93% accuracy; obfuscated URLs 40% accuracy

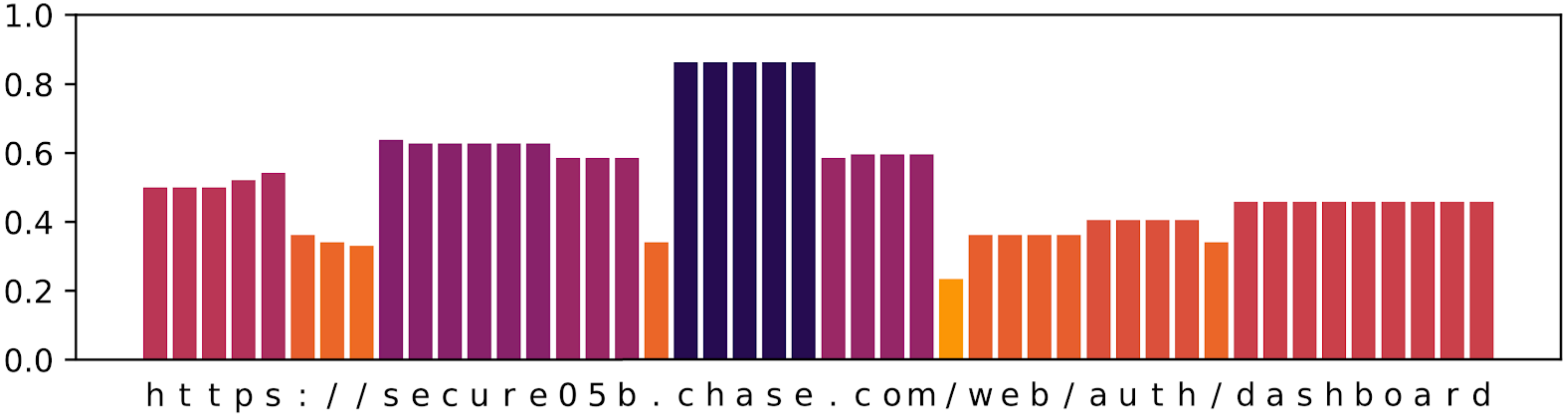
Obfuscation	Example	Accuracy
None (Control)	https://example.com/login	93%
Typosquatting	https://exemple.com/login	70%
IDN Homograph	https://ежамple.com/login	53%
Self-Declared Secure	https://secure-example.com/login	36%
Fake ID in Credentials	https://example.com@a4930.nz/login	32%
URL Encoding Hides Subdomain as Domain	https://example.com%2e2x-log.in	29%
Long Subdomain Chain	https://example.com.0jg094.05930.3590902sdg9f0.249905930.3590902sdg.mx/login	26%

Observed Parsing Strategies

"... highlight each group of characters that helps you learn the identity of the website it points to"

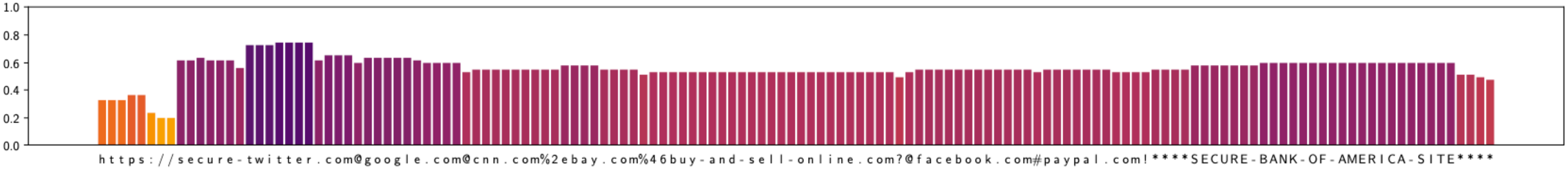






Observed Parsing Strategies

“... highlight each group of characters that helps you learn the identity of the website it points to”



https://secure-twitter.com@google.com@cnn.com%2ebay.com%46buy-and-sell-online.com?@facebook.com#paypal.com ****SECURE-BANK-OF-AMERICA-SITE****

Evaluation Strategies

“When you see a link/URL, how do you decide if it is safe to go there?”

Check for HTTPS

“I know it is safe when it reads https, the s stands for secure for me.”

“I first think about if it is a place I know is a legit website. Then I’m looking for HTTPS cert and if the URL just look sensible.”

Evaluation Strategies

“When you see a link/URL, how do you decide if it is safe to go there?”

Check for HTTPS

Familiarity

“I check the url for familiarity. It’s quite frankly easy to tell if it’s an official link to an authentic website.”

“…Like if I’m opening company A and the URL is companyA.com/... I would click it.”

Evaluation Strategies

“When you see a link/URL, how do you decide if it is safe to go there?”

Check for HTTPS

Familiarity

URL fields

“Check to see if it’s mispelled [sic] or weird”

“If it looks like crazy letters then I don’t click it”

“...Also check the prefix of the site and the domain of it. .com .org .ru things of that nature"

Evaluation Strategies

“When you see a link/URL, how do you decide if it is safe to go there?”

Check for HTTPS

Familiarity

URL fields

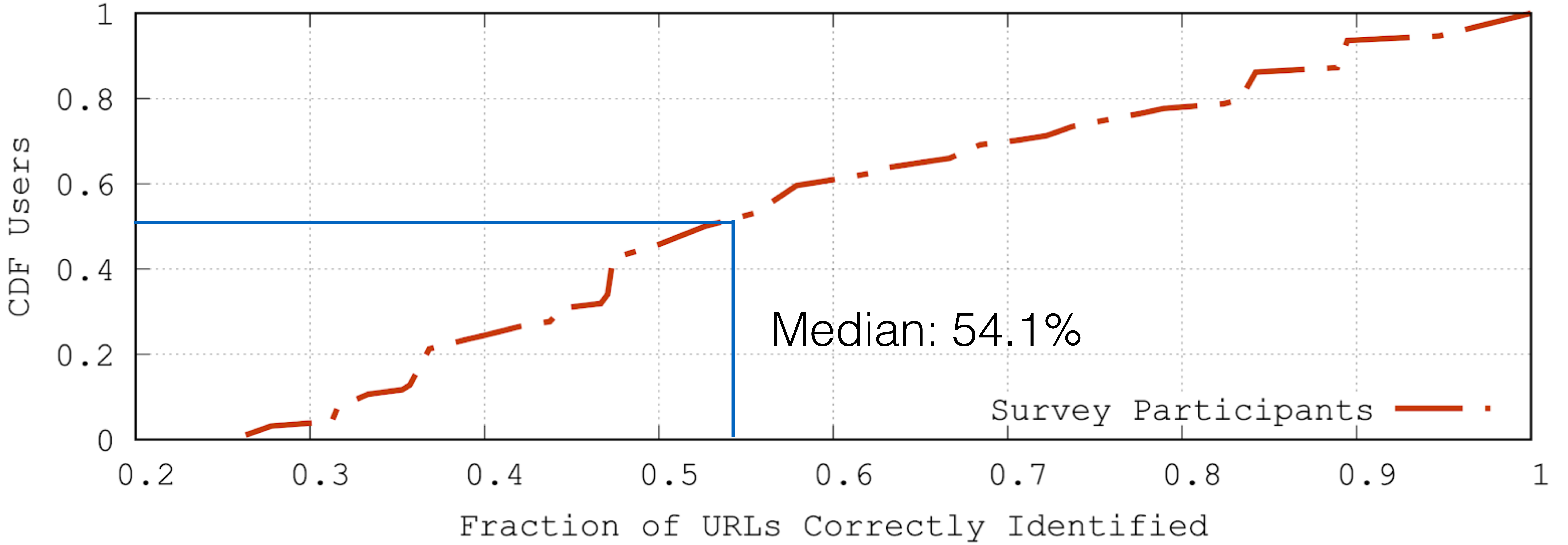
External tools/context

“i have a antivirus scanner, so it will check whether the site is safe or unsafe.”

“I consider the context of how it was presented to me. Sketchy email? No thanks. Someone spams a shortened link on a forum advertising something that’s too good to be true? No thanks.”

Target Identification

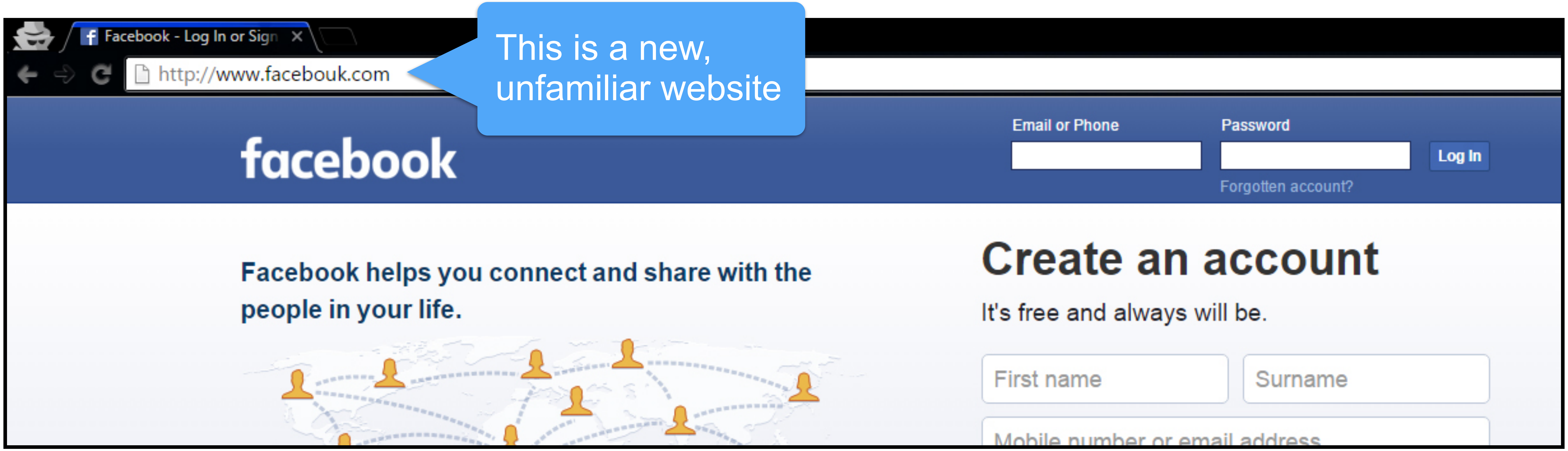
Asked users to describe the target of 19-20 URLs, some with one of 13 different URL obfuscations applied



Making URLs More Usable

Solutions that work without changing ubiquitous URLs?

Automated familiarity tracking



This is a new, unfamiliar website

Facebook - Log In or Sign

http://www.facebouk.com

facebook

Email or Phone

Password

Log In

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name

Surname

Mobile number or email address

Making URLs More Usable

Solutions that work without changing ubiquitous URLs?

Automated familiarity tracking

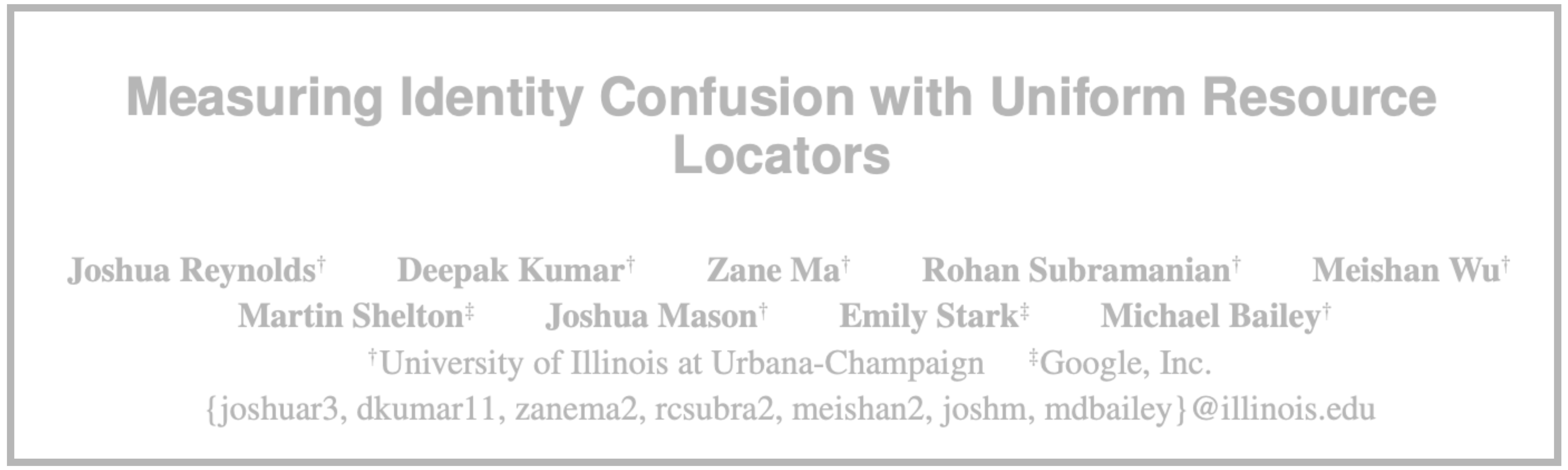
Alternate URL presentations

https://paypal.com.accounts.ggle.com

https://com.ggle.accounts.com.paypal

Phishing: Root Causes

Mistaken Identity



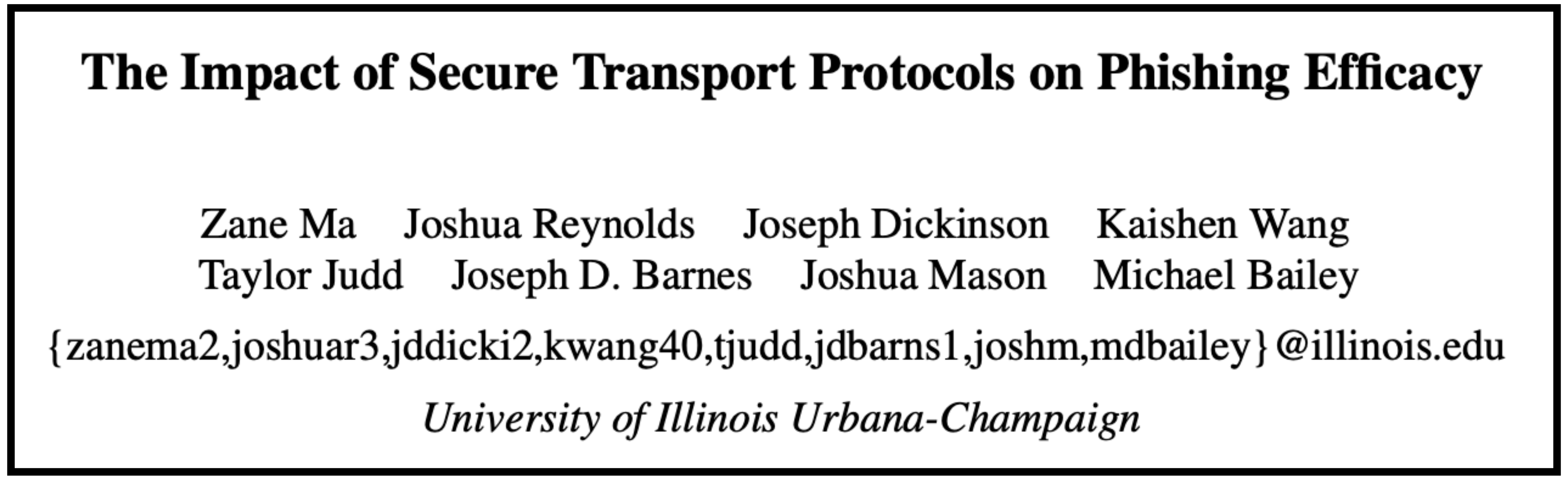
Measuring Identity Confusion with Uniform Resource Locators

Joshua Reynolds[†] Deepak Kumar[†] Zane Ma[†] Rohan Subramanian[†] Meishan Wu[†]
Martin Shelton[‡] Joshua Mason[†] Emily Stark[‡] Michael Bailey[†]
[†]University of Illinois at Urbana-Champaign [‡]Google, Inc.
{joshuar3, dkumar11, zanema2, rcsubra2, meishan2, joshm, mdbailey}@illinois.edu

CHI 2020

URL complexity leads to mistaken identity

Misplaced Trust



The Impact of Secure Transport Protocols on Phishing Efficacy

Zane Ma Joshua Reynolds Joseph Dickinson Kaishen Wang
Taylor Judd Joseph D. Barnes Joshua Mason Michael Bailey
{zanema2,joshuar3,jddicki2,kwang40,tjudd,jdbarns1,joshm,mdbailey}@illinois.edu
University of Illinois Urbana-Champaign

CSET 2019

Users may (mis)place trust in HTTPS

Existing Security Protocols Lack Trustworthiness

Not designed to protect against phishing

TLS = Confidentiality + Integrity + Identity/Authenticity

TLS secures connections, not content

Prior work:

1. Some users look at connection security indicators when exposed to phishing

2. Users confuse “connection security” and “site security”

Experimental Goals

1. Does the presence of secure transport protocols make phishing more effective?

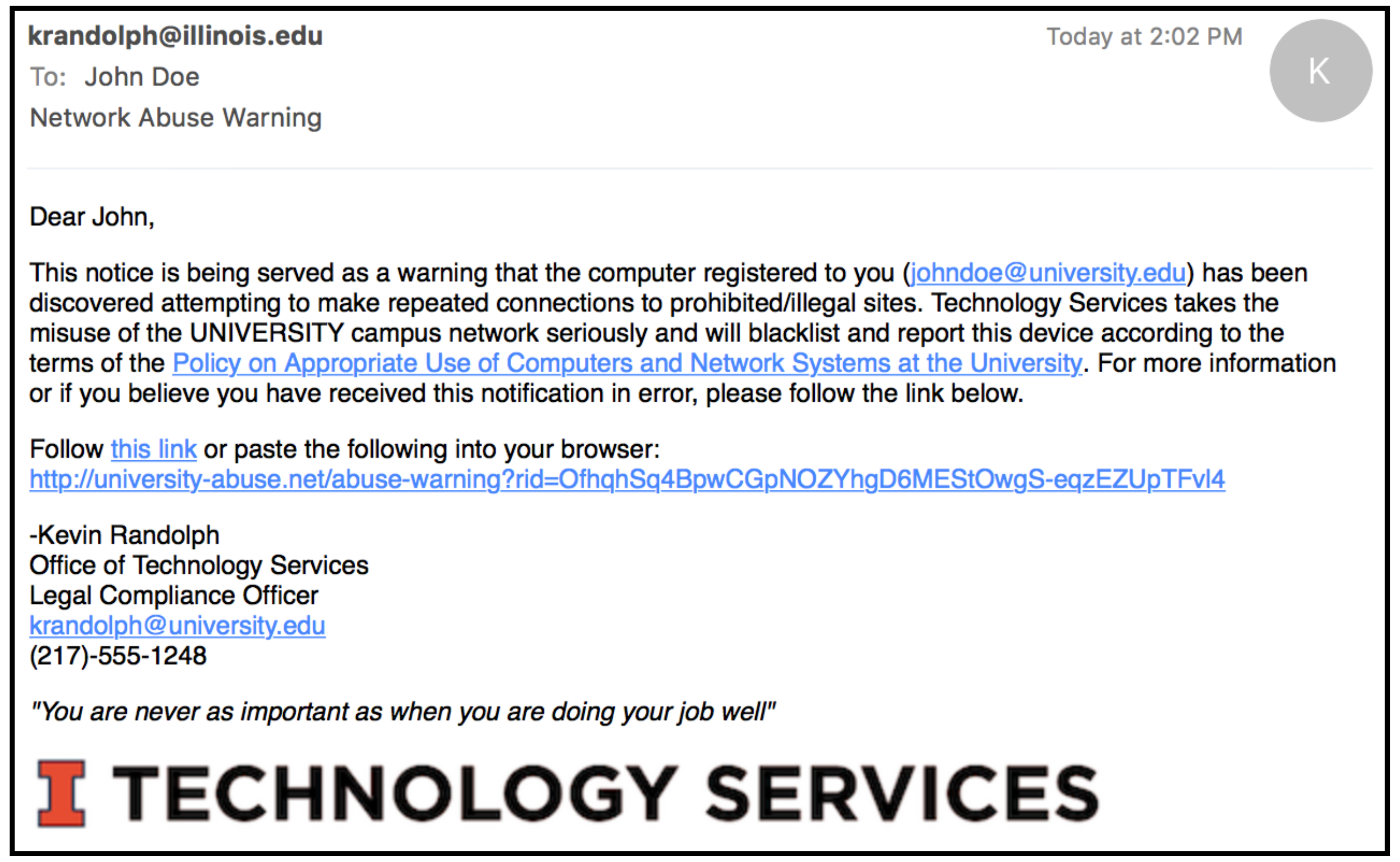
   Methodology: A/B test HTTP/HTTPS and SMTP/SMTP+TLS

2. Does browser URL bar UI (e.g. security indicators) influence phishing susceptibility?

   Methodology: Generate and feature code browser screenshots, correlate URL bar features with phishing outcomes

Phishing Experiment

1. Open Email



krandolph@illinois.edu Today at 2:02 PM
To: John Doe
Network Abuse Warning

Dear John,

This notice is being served as a warning that the computer registered to you (johndoe@university.edu) has been discovered attempting to make repeated connections to prohibited/illegal sites. Technology Services takes the misuse of the UNIVERSITY campus network seriously and will blacklist and report this device according to the terms of the Policy on Appropriate Use of Computers and Network Systems at the University. For more information or if you believe you have received this notification in error, please follow the link below.

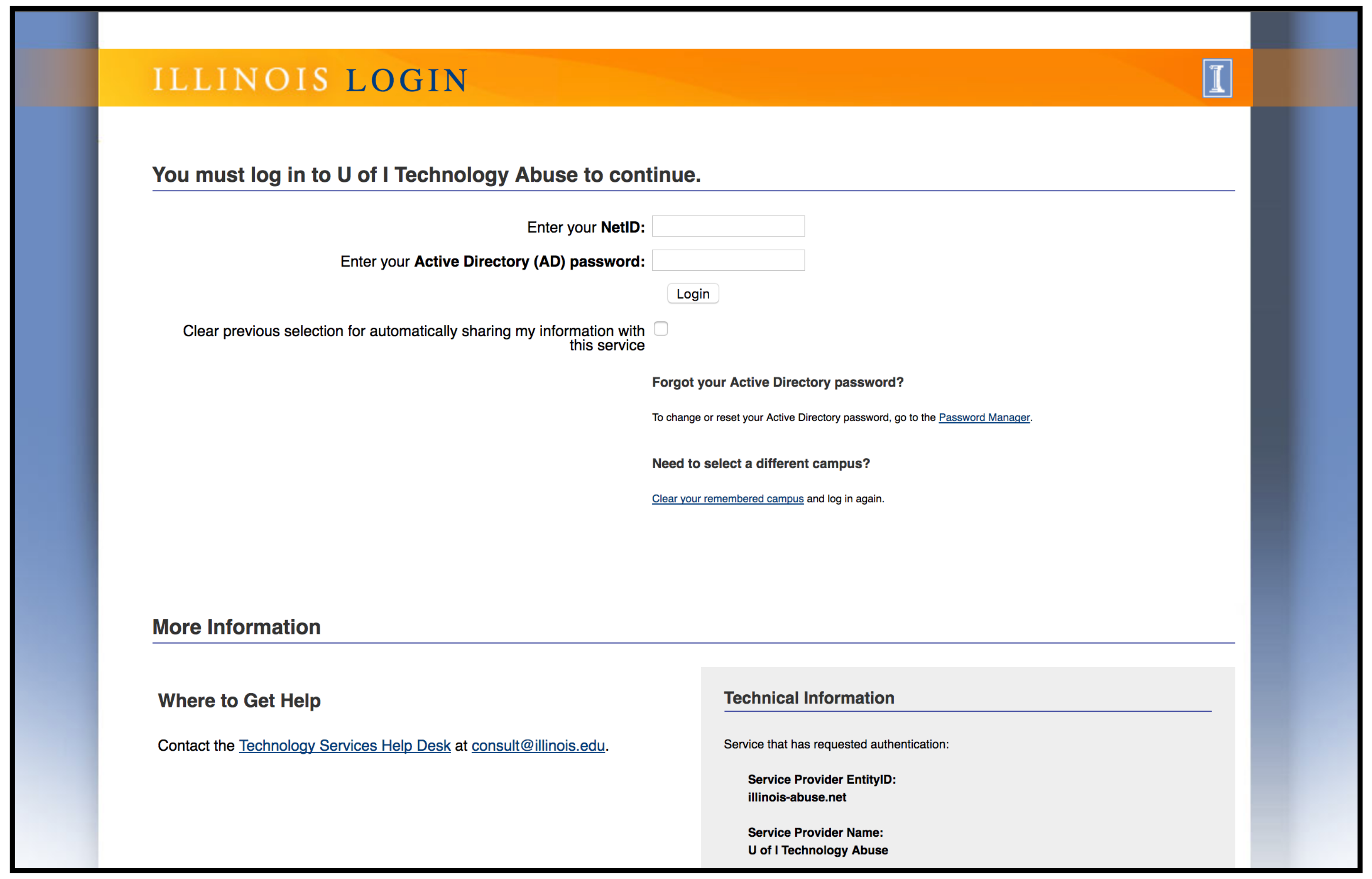
Follow this link or paste the following into your browser:
http://university-abuse.net/abuse-warning?rid=OfhqhSq4BpwCGpNOZYhgD6MEStOwgS-eqzEZUpTFvl4

-Kevin Randolph
Office of Technology Services
Legal Compliance Officer
krandolph@university.edu
(217)-555-1248

"You are never as important as when you are doing your job well"

TECHNOLOGY SERVICES

2. Access Site



ILLINOIS LOGIN

You must log in to U of I Technology Abuse to continue.

Enter your **NetID:**

Enter your **Active Directory (AD) password:**

Clear previous selection for automatically sharing my information with this service □

Forgot your Active Directory password?

To change or reset your Active Directory password, go to the Password Manager.

Need to select a different campus?

Clear your remembered campus and log in again.

More Information

Where to Get Help

Contact the Technology Services Help Desk at consult@illinois.edu.

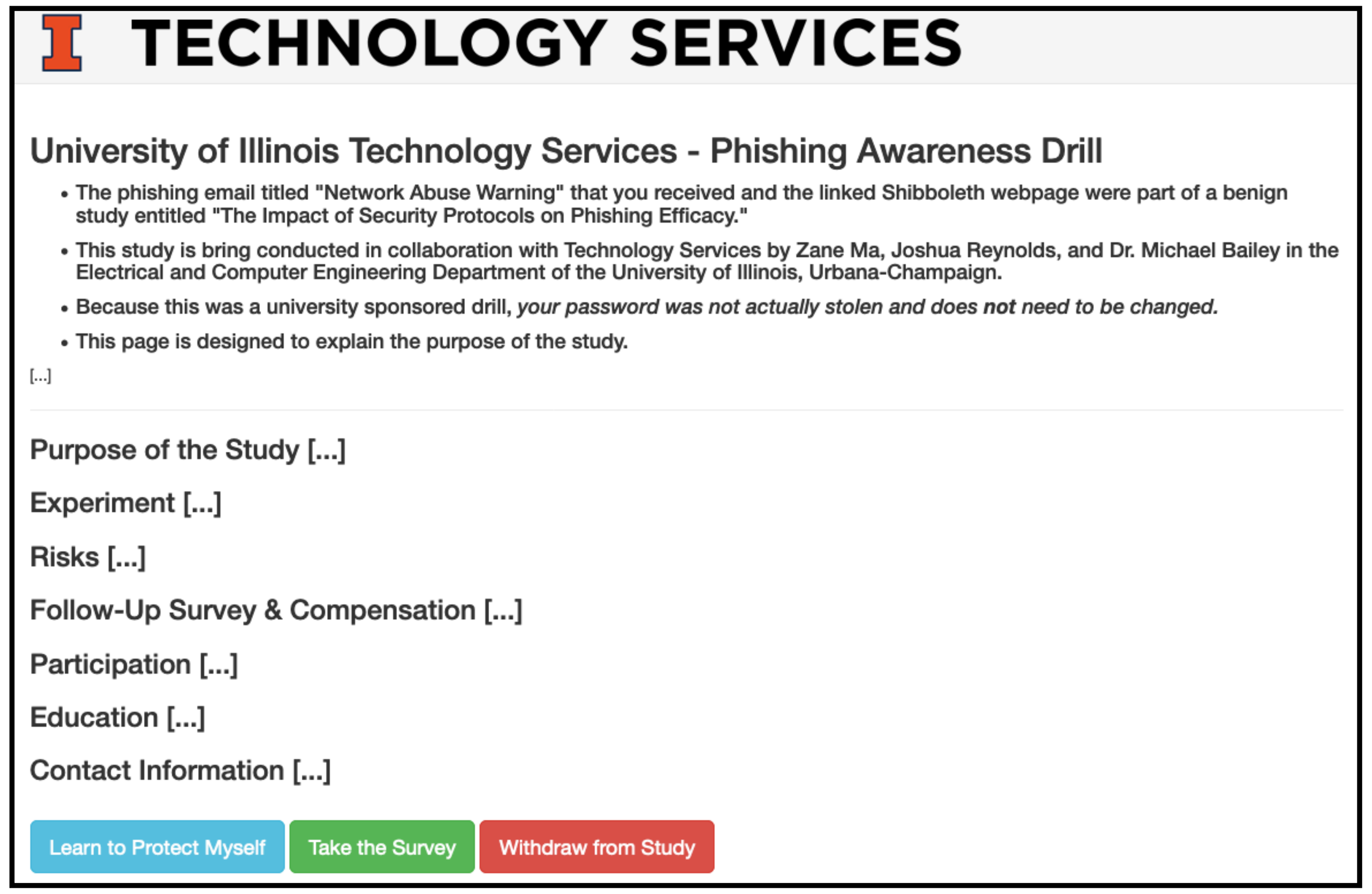
Technical Information

Service that has requested authentication:

Service Provider EntityID:
illinois-abuse.net

Service Provider Name:
U of I Technology Abuse

3. Submit Credentials



TECHNOLOGY SERVICES

University of Illinois Technology Services - Phishing Awareness Drill

- The phishing email titled "Network Abuse Warning" that you received and the linked Shibboleth webpage were part of a benign study entitled "The Impact of Security Protocols on Phishing Efficacy."
- This study is bring conducted in collaboration with Technology Services by Zane Ma, Joshua Reynolds, and Dr. Michael Bailey in the Electrical and Computer Engineering Department of the University of Illinois, Urbana-Champaign.
- Because this was a university sponsored drill, *your password was not actually stolen and does **not** need to be changed.*
- This page is designed to explain the purpose of the study.

[...]

Purpose of the Study [...]

Experiment [...]

Risks [...]

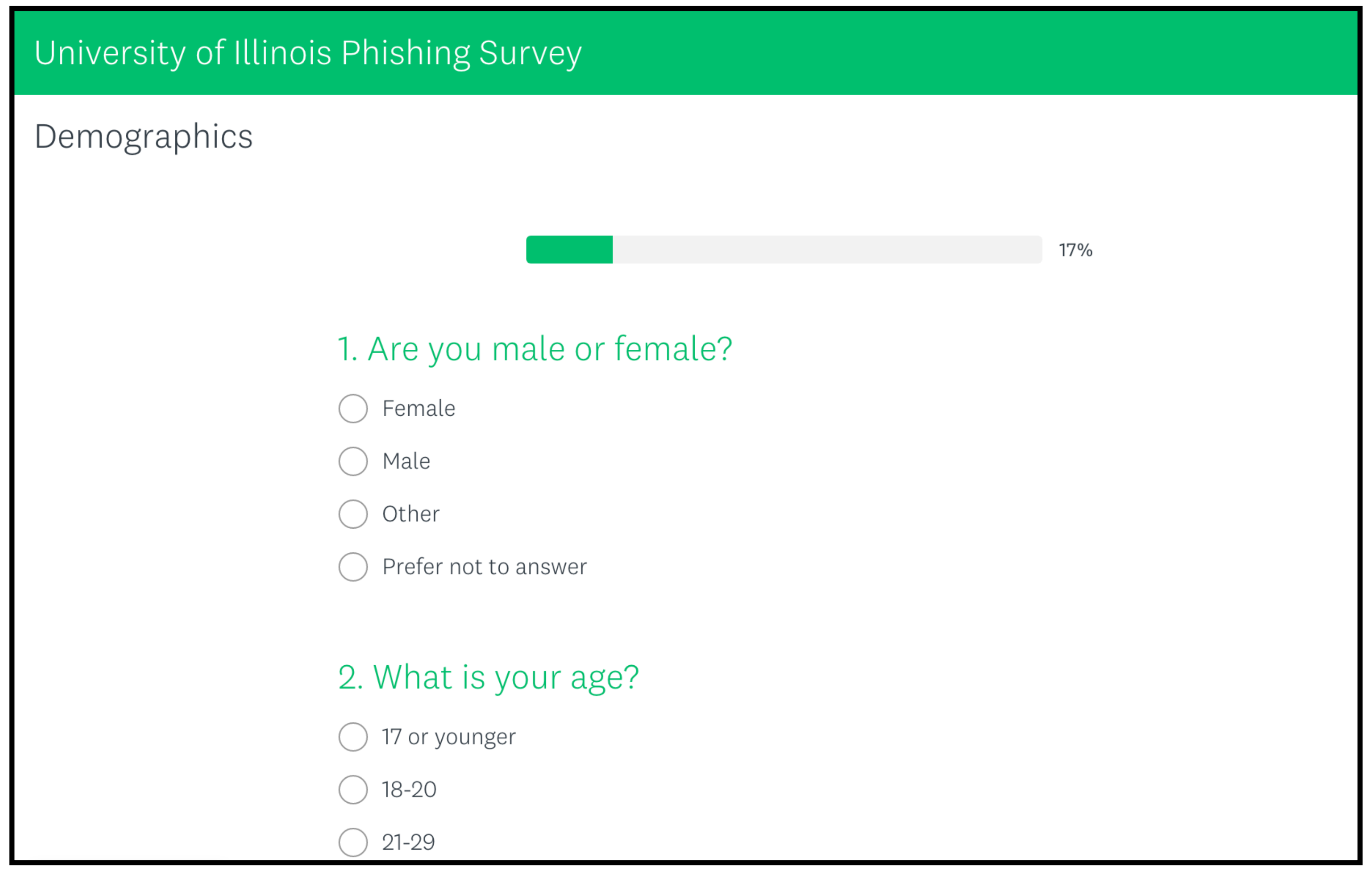
Follow-Up Survey & Compensation [...]

Participation [...]

Education [...]

Contact Information [...]

4. Opt-In To Survey



University of Illinois Phishing Survey

Demographics

1. Are you male or female?

○ Female
○ Male
○ Other
○ Prefer not to answer

2. What is your age?

○ 17 or younger
○ 18-20
○ 21-29

Phishing Campaign

Target population: 266 employees of a university IT organization

0. Send Email	1. Open Email	2. Access Site	3. Submit Credentials
266 Users	140 Users	92 Users	57 Users
100%	53%	35%	21%

Q1: Phishing Effectiveness

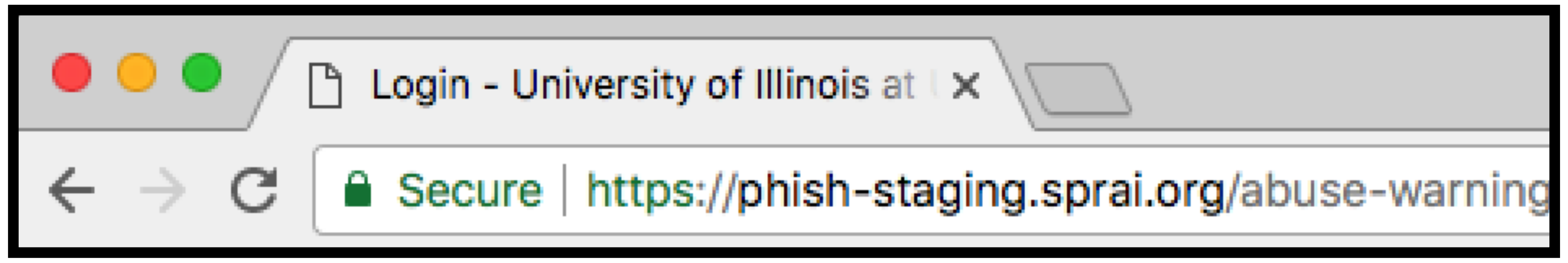
	2. Access Site		3. Enter Credentials	
HTTP	45/75 = 60.0%	p = 0.17	25/45 = 55.6%	p = 0.31
HTTPS	47/65 = 72.3%		32/47 = 68.0%	
TLS Email	45/71 = 63.3%	**p = 0.96**	30/47 = 63.8%	**p = 0.87**
No TLS Email	45/69 = 65.2%		27/45 = 60.0%	

Q2: Browser UI Correlation

Feature coded 2,882 screenshots across different browsers / platforms / OS

Correlate features with HTTP User-Agent for susceptible users

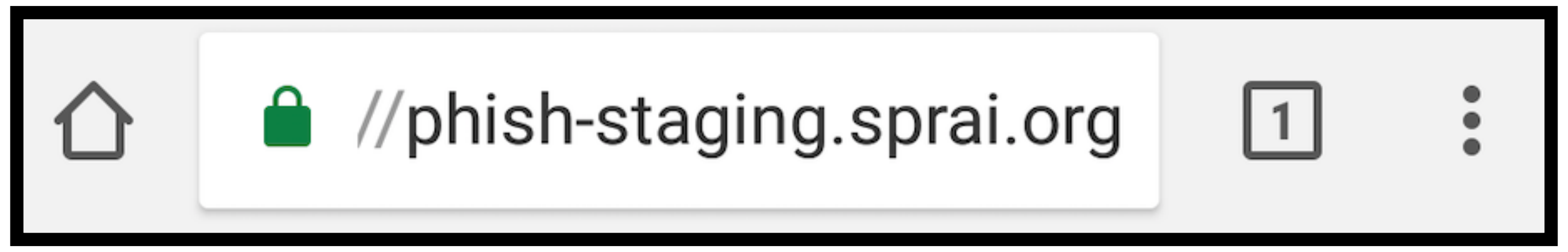
Mac 10.13 Chrome 63



Login - University of Illinois at

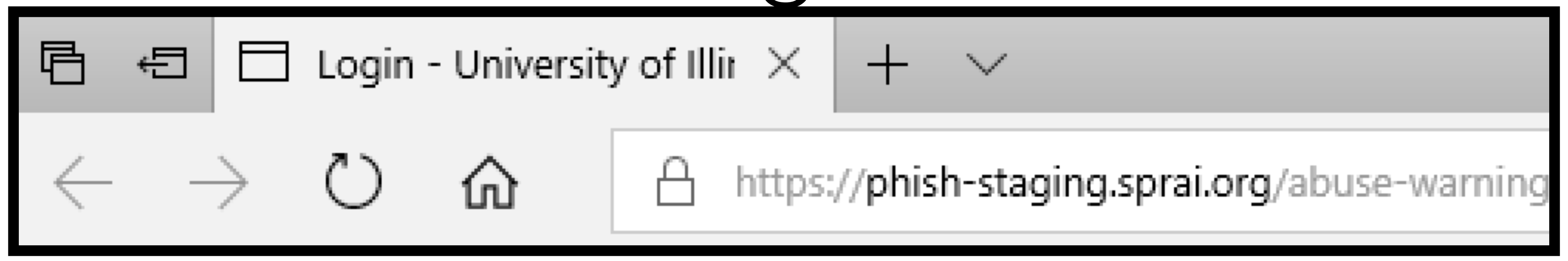
Secure | https://phish-staging.sprai.org/abuse-warning

Galaxy S7 Android 70 Mbl. Chrome 63



//phish-staging.sprai.org

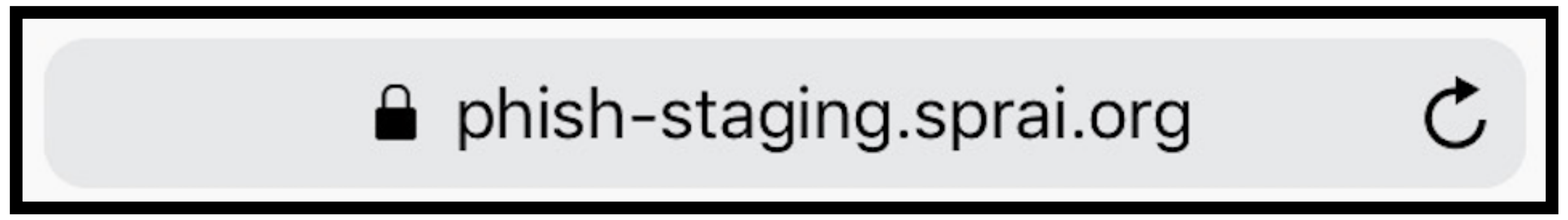
Windows 10 Edge 16



Login - University of Illir

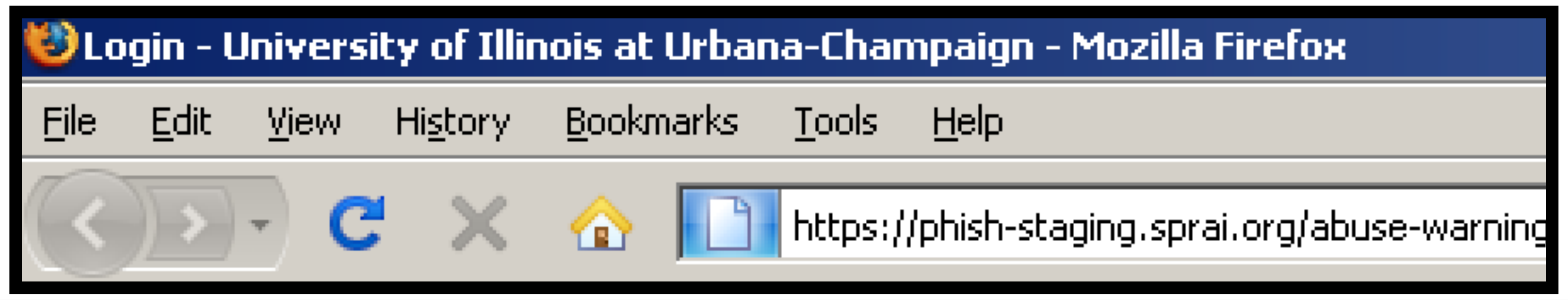
https://phish-staging.sprai.org/abuse-warning

iPhone 8 iOS 11 Mbl Safari 11.0



phish-staging.sprai.org

Windows XP SP2 Firefox 3.0



Login - University of Illinois at Urbana-Champaign - Mozilla Firefox

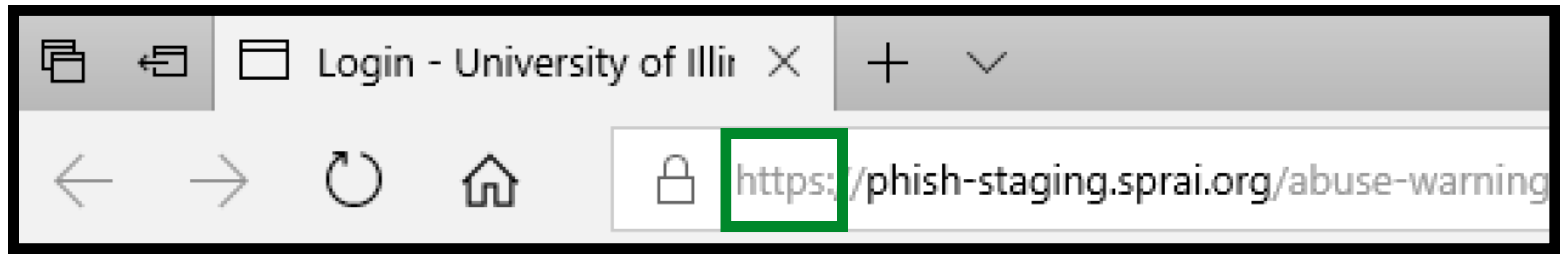
https://phish-staging.sprai.org/abuse-warning

https://github.com/teamnsrg/url-bar-coding

Q2: Browser UI Correlation

Feature	p_{exp}
Any Icon?	0.25
Lock Icon?	0.32
Lock Position	0.98
Lock Color	0.55
Detailed Lock?	0.54
Lock Additions	0.27
Favicon?	0.56
Favicon Position	0.32
Default Favicon	0.06
Protocol Visible?	0.07
Protocol Emphasis	0.63
Additional Text?	0.62
Add. Text Emphasis	0.62
Add. Text Background	0.97
Icon/URL Separator?	0.42

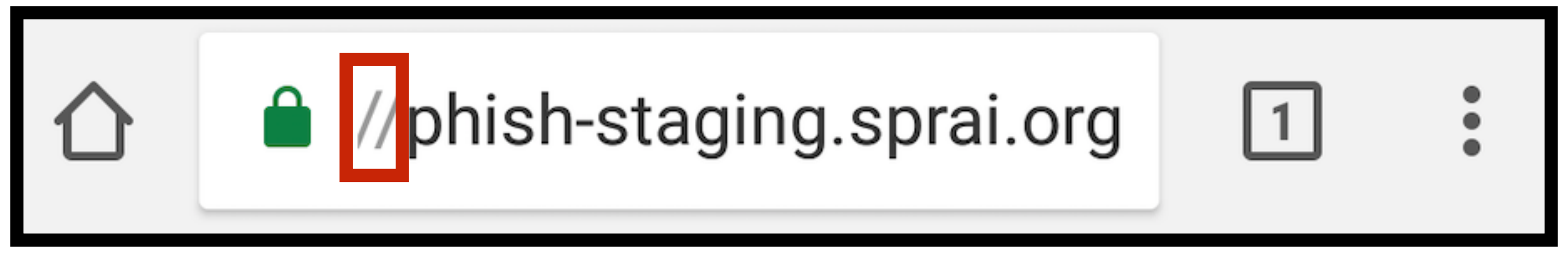
14/16 = 87.5% of users who saw protocol submitted credentials



Login - University of Illi

https://phish-staging.sprai.org/abuse-warning

27/46 = 58.7% of users who did not see protocol submitted credentials

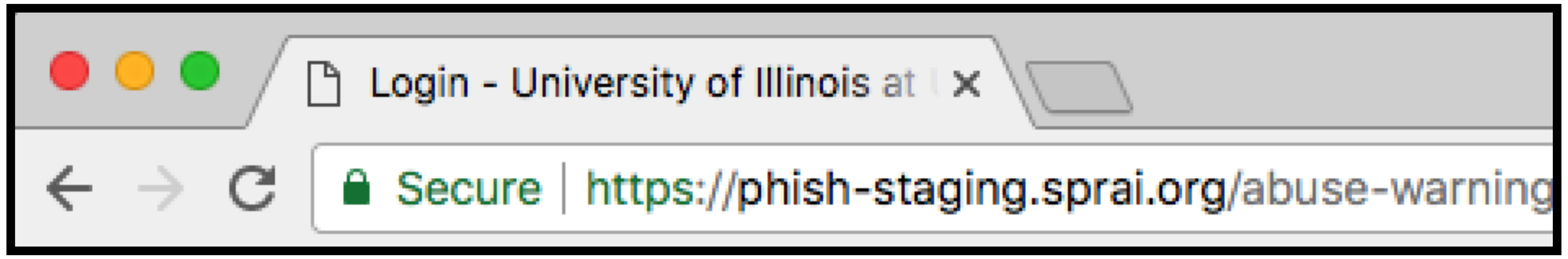


//phish-staging.sprai.org

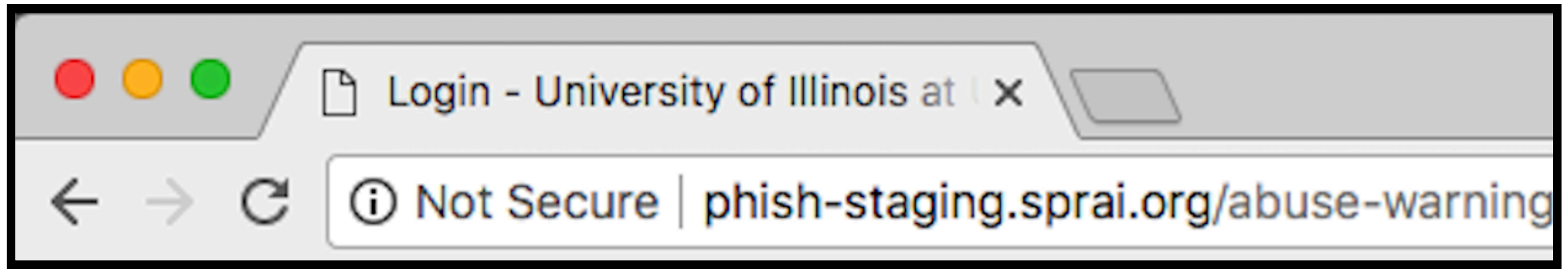
Q2: Browser UI Correlation

Feature	p_{exp}
Any Icon?	0.25
Lock Icon?	0.32
Lock Position	0.98
Lock Color	0.55
Detailed Lock?	0.54
Lock Additions	0.27
Favicon?	0.56
Favicon Position	0.32
Default Favicon	0.06
Protocol Visible?	0.07
Protocol Emphasis	0.63
Additional Text?	0.62
Add. Text Emphasis	0.62
Add. Text Background	0.97
Icon/URL Separator?	0.42

9/10 “Secure” submitted credentials


Login - University of Illinois at
Secure | https://phish-staging.sprai.org/abuse-warning

8/10 “Not Secure” submitted credentials


Login - University of Illinois at
Not Secure | phish-staging.sprai.org/abuse-warning

Takeaways

- The presence of HTTPS in phishing tended to increase effectiveness, but…need more data, more diverse target population
- Protocol presence may increase phishing susceptibility, while “Secure/Not Secure” had minimal distinction
- Another hint that users conflate credibility/trustworthiness with connection security

Collaborators

Michael Bailey

Josh Mason

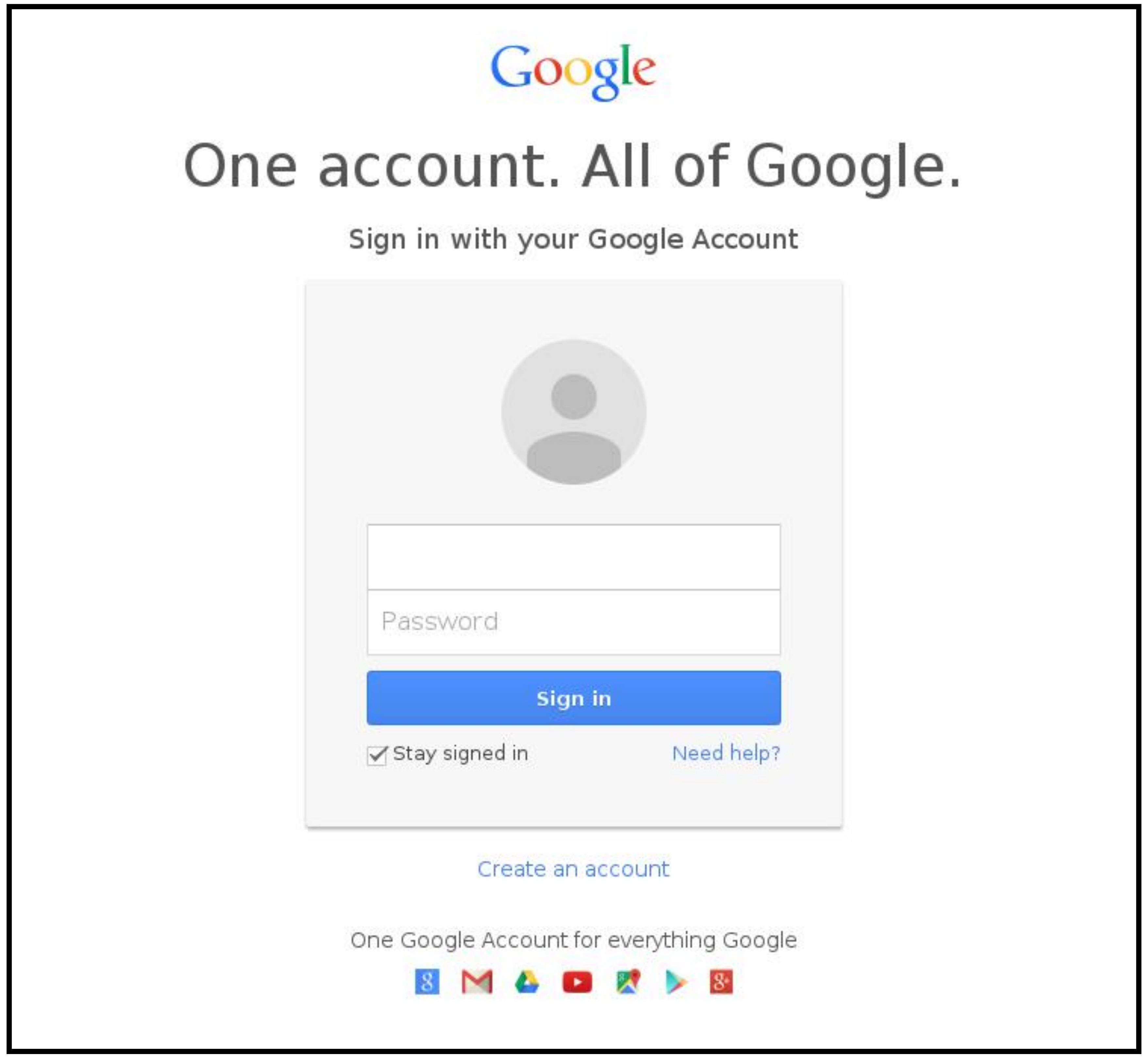
Deepak Kumar

Joshua Reynolds

Not pictured: Martin Shelton, Emily Stark, Kaishen Wang, Joseph Dickinson, Rohan Subramanian, Meishan Wu, Illinois Tech Services

Phishing: Root Causes

Mistaken Identity



Google

One account. All of Google.

Sign in with your Google Account

Password

Sign in

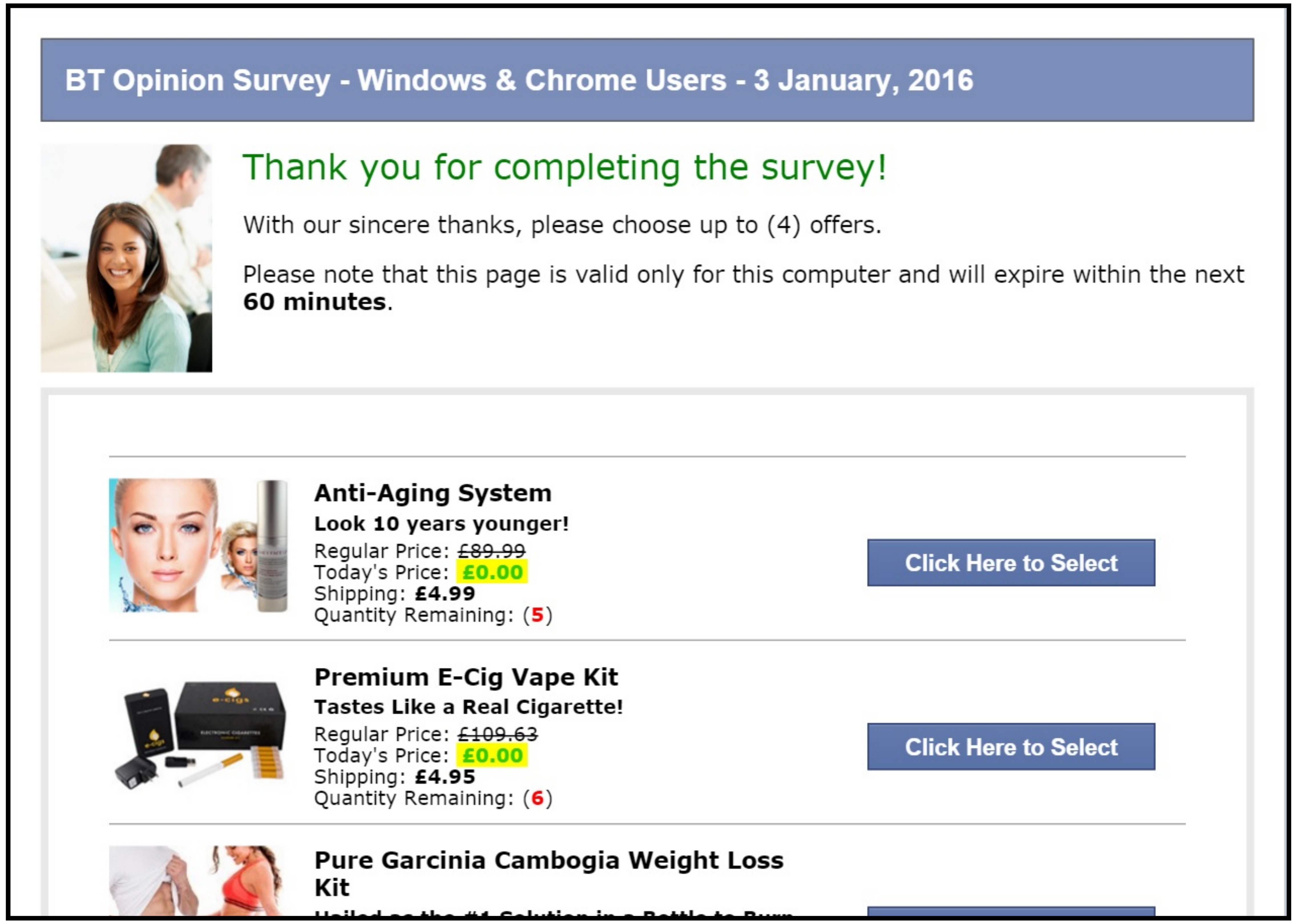
☑ Stay signed in   Need help?

Create an account

One Google Account for everything Google

accoounts-google.com

Misplaced Trust



BT Opinion Survey - Windows & Chrome Users - 3 January, 2016

Thank you for completing the survey!

With our sincere thanks, please choose up to (4) offers.

Please note that this page is valid only for this computer and will expire within the next **60 minutes**.

Anti-Aging System
Look 10 years younger!
Regular Price: ~~£89.99~~
Today's Price: **£0.00**
Shipping: **£4.99**
Quantity Remaining: (**5**)

Click Here to Select

Premium E-Cig Vape Kit
Tastes Like a Real Cigarette!
Regular Price: ~~£109.63~~
Today's Price: **£0.00**
Shipping: **£4.95**
Quantity Remaining: (**6**)

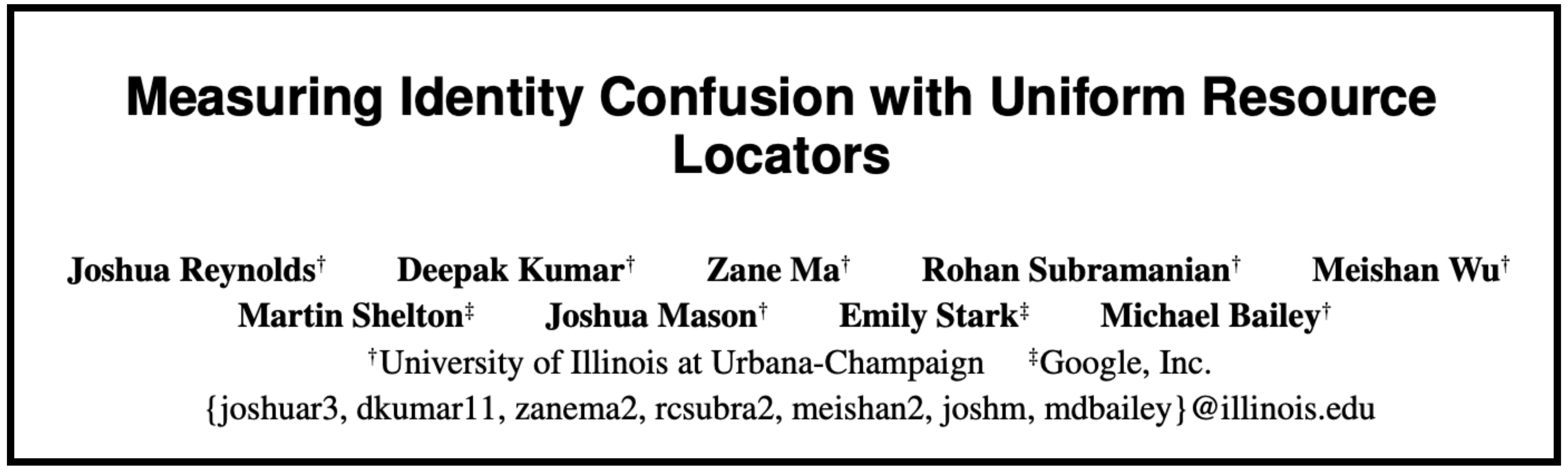
Click Here to Select

Pure Garcinia Cambogia Weight Loss Kit

questionsaboutisps.com

Phishing: Root Causes

Mistaken Identity



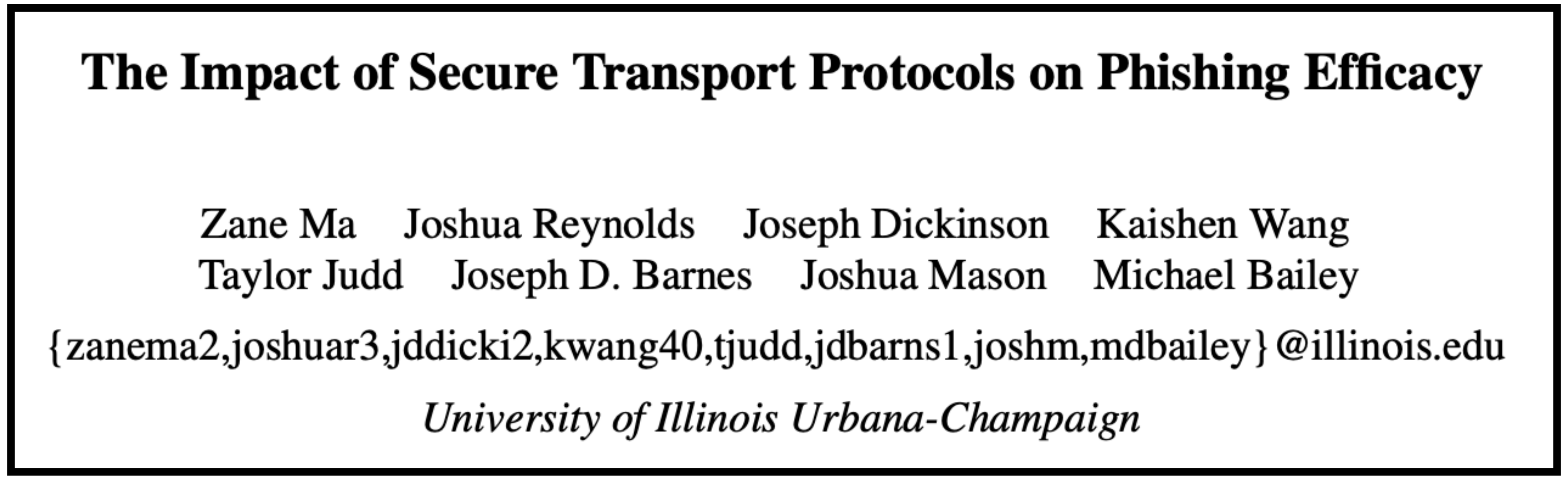
Measuring Identity Confusion with Uniform Resource Locators

Joshua Reynolds[†] **Deepak Kumar**[†] **Zane Ma**[†] **Rohan Subramanian**[†] **Meishan Wu**[†]
Martin Shelton[‡] **Joshua Mason**[†] **Emily Stark**[‡] **Michael Bailey**[†]
[†]University of Illinois at Urbana-Champaign [‡]Google, Inc.
{joshuar3, dkumar11, zanema2, rcsubra2, meishan2, joshm, mdbailey}@illinois.edu

CHI 2020

URL complexity leads to mistaken identity

Misplaced Trust



The Impact of Secure Transport Protocols on Phishing Efficacy

Zane Ma Joshua Reynolds Joseph Dickinson Kaishen Wang
Taylor Judd Joseph D. Barnes Joshua Mason Michael Bailey
{zanema2,joshuar3,jddicki2,kwang40,tjudd,jdbarns1,joshm,mdbailey}@illinois.edu
University of Illinois Urbana-Champaign

CSET 2019

Users may (mis)place trust in HTTPS

Fundamentals of Phishing: A Usability Perspective

Zane Ma

University of Illinois Urbana-Champaign

zanema2@illinois.edu
https://zanema.com